NEC

GVT-245342-001-00 1.7

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

改版履歴

版数	日付	改版内容
1.0	2024/08	初版発行
1.1	2024/11	・「03-システム管理」の「1 章 装置管理」の以下のコマンドの説明を更新しました。 **・diag boot-info display** ・「05-ネットワーク接続」の「19 章-HTTP」に下記のコマンドを追加しました。 **・http-redirect https-rate-limit** ・「12-WLAN アドバンスド機能」の「3 章 IoT 機能の設定」に下記のコマンドを追加しました。 **・rfid-tracking mode** **・rfid-tracking radio** **・display wlan rfid-tracking radio** ・誤記訂正
1.2	2025/03	・「13-ユーザアクセスと認証」の「3 章 AAA」の以下のコマンドの説明を更新しました。 **・local-user**

版数	日付	改版内容
1.3	2025/09	・「02-基本機能」の「3 章 ログイン管理」に下記コマンドを追加しました。 **・http url allowlist** ・「03-システム管理」の「1 章 装置管理」に下記コマンドを追加しました。 **・locator blink** **・user-role** ・「03-システム管理」の「5 章 Information Center」に下記コマンドを追加しました。 **・info-center loghost keep-alive custom-info** **・info-center loghost keep-alive enable** **・info-center loghost keep-alive interval** **・info-center loghost keep-alive level** ・「06 WLAN アクセス」の「1 章 WLAN アクセス」の下記コマンドで **frequency-band 6** のパラメータをサポートしました。 **・display wlan client** ・「07-AP 管理」に「2 章 コンフィグレーションプロファイルの設定」の章を追加しました。 ・「08-WLAN セキュリティ」の「1 章 WLAN セキュリティ」の下記コマンドで **enterprise-only-mode** と **enterprise-transition-mode** のパラメータをサポートしました。 **・wpa3** ・「09-無線管理」の「1 章 無線管理」に下記コマンドを追加しました。 **・wlan multiple-bssid enable** **・wlan in-band 6g-discovery** ・「09-無線管理」の「1 章 無線管理」の下記コマンドに 802.11abe と 802.11gbe での利用についてのメモ書きを追加しました。 **・dot11g protection** **・dot11n protection** ・「12-WLAN アドバンスド機能」の「1 章 WLAN 最適化」に下記コマンドを追加しました。 **・rrop flow-schedule-mode** **・option keep-active** ・「12-WLAN アドバンスド機能」に「4 章 HotSpot2.0 の設定」の章を追加しました。 ・「13-ユーザアクセスと認証」の「2 章 WLAN IP スヌーピング」に下記コマンドを追加しました。 **・display wlan statistics client-ip-conflict** ・誤記訂正

版数	日付	改版内容
1.4	2026/02	・「03-システム管理」の「1 章 装置管理」に下記コマンドを追加しました。 **・restore factory-default** ・「03-システム管理」の「5 章 Information Center」の下記コマンドのデフォルト値を修正しました。 **・info-center logbuffer size** ・「05-ネットワーク接続」の「2 章 リンクアグリゲーション」の下記コマンドを追加しました。 **・link-aggregation-mode** ・「05-ネットワーク接続」の「6 章 LLDP」の下記コマンドの表示情報の説明表を修正しました。 **・display lldp local-information** ・「06-WLAN アクセス」の「1 章 WLAN アクセス」の下記コマンドのデフォルト値とパラメータの説明を修正しました。 **・client forwarding-location** ・「06-WLAN アクセス」の「1 章 WLAN アクセス」の下記コマンドのコマンド出力表を修正しました。 **・display wlan client** ・「06-WLAN アクセス」の「1 章 WLAN アクセス」の下記コマンドのコマンド出力表を修正しました。 **・display wlan client status** ・「08-WLAN セキュリティ」の「1 章 WLAN セキュリティ」の下記コマンドにメモ欄を追記しました。 **・preshared-key** ・「08-WLAN セキュリティ」の「2 章 WIPS 設定コマンド」に下記コマンドを追記しました。 **・wips enable** ・「08-WLAN セキュリティ」の「2 章 WIPS 設定コマンド」の下記コマンドの view を修正しました。 **・wips virtual-security domain** ・「12-WLAN アドバンスド機能」の「1 章 WLAN 最適化」に下記コマンドを追記しました。 **・option client hide-node protection** ・「12-WLAN アドバンスド機能」の「1 章 WLAN 最適化」の下記コマンドのデフォルト値を修正し、パラメータ値の記載を削除しました。 **・option keep-active** ・「14-高可用性」の「1 章 WLAN 高可用性」の下記コマンドを修正しました。 **・wlan ap-backup hot-backup enable** ・「14-高可用性」の「3 章 CloudCluster」の下記コマンドの説明を修正ました。 **・mad enable**

版数	日付	改版内容
		・「17-ネットワーク管理」の「10 章 Netmeister」の下記コマンドの説明を修正しました。 ・**netmeister alarm enable notice**
1.5	2026/04	・「03-システム管理」の「5 章 Information Center」の下記コマンドのデフォルト値の記載を更新しました。 ・**info-center loghost keep-alive enable** ・「08-WLAN セキュリティ」の「1 章 WLAN セキュリティ」に下記のコマンドを追加しました。 ・**enhanced-open enable** ・**enhanced-open transition-mode service-template** ・「12-WLAN アドバンスド機能」の「3 章 IoT 機能の設定」に「BLE 機能の設定コマンド」と「サーバへの IoT データのレポート設定コマンド」を追加しました。 ・「13-ユーザアクセスと認証」の「3 章 AAA」に「EAP プロファイル設定コマンド」と「RADIUS サーバ設定コマンド」を追加しました。 ・「17-ネットワーク管理と監視」の「10 章 NetMeister」に下記コマンドを追加しました。 ・**netmeister event syslog enable** 誤記訂正
1.6	2026/07	・「06-WLAN アクセス」の「1 章 WLAN アクセス」の下記コマンドに、6GHz 無線に関する注記を追加しました。 ・**beacon ssid-hide** ・「08-WLAN セキュリティ」の「WIPS の設定」に、無線通信と WIPS センサの併用に関して説明を追加しました。 ・「13-ユーザアクセスと認証」の「2 章 WLAN IP スヌーピング」に下記コマンドを追加しました。 ・**wlan client ip-conflict-detection enable** 誤記訂正
1.7	2026/10	・「02-基本機能」の「1 章 CLI」に、下記コマンドを追加しました。 ・**repeat** ・「03-システム管理」の「3 章 ハードウェアリソース管理」に、下記コマンドを追加しました。 ・**display transceiver alarm** ・**display transceiver diagnosis** ・**display transceiver manuinfo** ・「08-WLAN セキュリティ」の「1 章 WLAN セキュリティ」の、**akm mode** コマンドの **private-psk** パラメータは未サポートであるため削除しました。

Copyright © NEC Corporation 2024-2026

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- 本装置は *QX-W2300AC シリーズアクセスコントローラ コマンドマニュアル*に記載されているコマンドのみ使用することができます。*QX-W2300AC シリーズアクセスコントローラ コマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

バージョン

本マニュアルに対応する製品バージョンは Version 9.4.x を含む以降のソフトウェアです。

関連マニュアル

次のマニュアルには、QX-W2300AC シリーズアクセスコントローラに関する詳細な説明があります

マニュアル	内容
QX-W2300AC シリーズアクセスコントローラ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-W2300AC シリーズアクセスコントローラ オペレーションマニュアル	機能の設定について説明しています。
QX-W2300AC シリーズアクセスコントローラ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-W2300AC シリーズアクセスコントローラ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-W シリーズ Web 認証(ポータル認証) オペレーションマニュアル	QX-W シリーズ の Web 認証 (ポータル認証)に関する設定について説明しています。
QX-W シリーズ Web 認証(ポータル認証) コマンドマニュアル	QX-W シリーズ の Web 認証 (ポータル認証)に関するコマンドについて説明しています。

マニュアルの構成

このコマンドマニュアルは以下のセクションで構成されます。

- **ライセンス管理**

  ライセンス管理の設定について説明します。

- **基本機能**

  装置へのアクセス方法、ファイルシステム管理、設定ファイル管理、ソフトウェア管理、装置管理といった、装置管理の設定について説明します。

- **システム管理**

  システム保守、ネットワーク管理の設定といった、Ethernet スイッチのシステム管理および保守について説明します。

- **インタフェース**

リンクアグリゲーション、VLAN、LLDP といった、レイヤ 2 機能の設定について説明します。

- **ネットワーク接続**

  ARP、IP アドレス（IPv4）、DHCP 関連機能、IP パフォーマンスといった、ネットワークプロトコルの設定について説明します。

- **WLAN アクセス**

  WLAN アクセスの設定について説明します。

- **AP 管理**

  AP 管理の設定について説明します。

- **WLAN セキュリティ**

  WLAN セキュリティ、WIPS の設定について説明します。

- **無線管理**

  ロードバランス、RRM などの無線管理の設定について説明します。

- **WLAN ローミング**

  WLAN ローミングの設定について説明します。

- **WLAN トラフィック最適化**

  WLAN トラフィックの最適化、アイソレーションの設定について説明します。

- **WLAN アドバンスド機能**

  WLAN メッシュ、IoT 機能の設定について説明します。

- **ユーザアクセスと認証**

  WLAN 認証などの設定について説明します。

- **高可用性**

  Track、クラウドクラスタの設定について説明します。

- **セキュリティ**

  ACL、AAA、RADIUS、SSH 等の設定について説明します。

- **QoS**

  QoS の設定について説明します。

- **ネットワーク管理と監視**

  システム保守、SNMP、NetMeister などのシステム管理および保守について説明します。

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンド表記規則

表記規則	説明
太字体	コマンドラインを示すキーワードには**太字体**を使用します。
イタリック体	コマンドの引数は*イタリック体*を使用します。
[ ]	大カッコに囲まれた項目(キーワード、引数)はオプションです。
{ x | y | … }	選択する項目は、中カッコに入れて縦線で区切ってあります。1 つを選択します。
[x | y | …]	オプションの選択項目は、大カッコに入れて縦線で区切ってあります。1 つまたは複数を選択します。
{ x | y | … }*	選択する項目は、中カッコに入れて縦線で区切ってあります。少なくとも 1 つ選択できます。
[x | y | …]*	オプションの選択項目は、大カッコに入れて、縦線で区切ってあります。1 つあるいは複数選択することも、何も選択しないこともできます。
&<1-n>	&の前のキーワードと引数を組み合わせます。引数で指定した数までキーワードを繰り返し指定できます。
#	#で始まる行はコメントを示します。

II. GUI 表記規則

表記規則	説明
< >	ボタン名は三角カッコに入っています。例えば、<OK>ボタンをクリックします。
[ ]	ウィンドウ名、メニュー項目、データ表、およびフィールド名は大カッコに入っています。例えば、[New User]ウィンドウが表示されます。
/	複数レベルのメニューはスラッシュで区切ってあります。例えば、[File/Create/Folder]。

III. キーボード操作

表記規則	説明
<KEY>	KEY のキーを押します。例えば、 <Enter>は Enter キーを押します。
<KEY1 + KEY2>	複数のキーを同時に押します。例えば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<KEY1, KEY2>	複数のキーを順番に押します。例えば、 <Alt, A>は 2 つのキーを順に押すことを表します。

IV. マウス操作

表記規則	説明
クリック	マウスのボタンを素早く押します。特に指定がない場合は左ボタンを押します。

表記規則	説明
ダブルクリック	マウスの左ボタンを素早く 2 回押します。
ドラッグ	マウスの左ボタンを押したまま移動します。

V. 記号

表記規則	説明
⚠ **警告**	表示を無視したり指示に従わない場合、利用者が怪我などをする恐れのある重要な情報を示します。
⚠ **注意**	表示を無視したり指示に従わない場合、データの損失や破損、ハードウェアやソフトウェアの損傷などが発生する恐れのある重要な情報を示します。
⚠ **重要**	注意を払う必要がある情報を示します。
🕮 **メモ**	追加または補足となる情報を示します。
🕮 **ポイント**	参考となる情報を示します。

VI. ネットワークアイコン

表記規則	説明
	ルータ、スイッチ、またはファイアウォールなどの一般的なネットワークデバイスを表しています。
	ルータまたはレイヤ 3 スイッチなどのルーティング対応のデバイスを表しています。
	レイヤ 2、レイヤ 3 スイッチまたはレイヤ 2 転送機能に対応したルータなどの一般的なスイッチデバイスを表しています。

VII. 設定例

本マニュアルの設定例は各機能での代表的な設定例を示します。インタフェース番号、システム名の表記、display コマンドで表示される情報は、ご使用の装置と異なることがあります。

VIII. セキュリティ強化

セキュリティ強化のため、simple で設定されたパスワードも cipher や hash で登録されます。

本マニュアルは以下に示す 17 個のセクションで構成されています。

01 - ライセンス管理

02 - 基本機能

03 - システム管理

04 - インタフェース

05 - ネットワーク接続

06 - WLAN アクセス

07 - AP 管理

08 - WLAN セキュリティ

09 - 無線管理

10 - WLAN ローミング

11 - WLAN トラフィック最適化

12 - WLAN アドバンスド機能

13 - ユーザアクセスと認証

14 - 高可用性

15 - セキュリティ

16 - QoS

17 -ネットワーク管理と監視

QX-W2300AC シリーズアクセスコントローラ

コマンドマニュアル

1. ライセンス管理

本マニュアルは以下に示す章で構成されています。

01-ライセンス管理

02-AP ライセンス管理

目次

このセクションのページは **1-x-x** です。

1 章 ライセンス管理 1-1
1.1 ライセンス管理コマンド 1-1
1.1.1 display license 1-1
1.1.2 display license device-id 1-3
1.1.3 display license feature 1-4
1.1.4 license activation-file install 1-5
1.1.5 license activation-file uninstall 1-7
1.1.6 license compress 1-8

1章 ライセンス管理

1.1 ライセンス管理コマンド

1.1.1 display license

Syntax

display license [*activation-file*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

activation-file：デバイス上のアクティブファイルの License に関する情報を表示します。

説明

display license コマンドで、ライセンス情報を表示します。

パラメータを指定しない場合、すべてのライセンス情報を表示します。

例

#すべてのライセンス情報を表示します。

<AC> display license

```
flash:/license/wx3510x.ak
Feature:APMGR
Product Description:Enhanced Access Controller License, 128 APs, for Verticals,
fo
r V 7
Registered at:2020-07-22 16:00:46
License Type:Trial (days restricted)
Trial Time Left (days):0
Current State:Expired

Pre-installed License
Feature:APMGR
Feature Description:PreAtom This is APMGR license
```

```
Time Left (days):0
Current State:Expired
```

表 1-1 コマンド出力

フィールド	説明
Feature	プロパティ名
Feature Description	プロパティの説明
Product Description	ライセンスの説明
Registered at	デバイスへのインストール時間
License Type	ライセンスタイプ。値は次のとおりです。 ● NA:Licenseのタイプを取得できません ● Permanent:永続的なタイプで、このライセンスが常に有効で、期限が切れないことを示します。 ● Days restricted: ライセンスがGAであり、30日間などの相対期間であることを示す相対時間タイプ。 ● Date restricted: ライセンスが正式にリリースされ、2015年5月1日から2015年5月30日までの絶対期間であることを示す絶対期間タイプ。 ● Trial (days restricted):相対時間タイプの評価ライセンス。これは、ライセンスが相対時間タイプの非公式リリースライセンスであることを示します。 Trial (date restricted):絶対タイムタイプのトライアルライセンスは、ライセンスが絶対タイムタイプの非公式リリースライセンスであることを示しています。
Time Left (days)	正式認可相対時間タイプのタイム・バランス
Trial Time Left (days)	一時的認可相対時間タイプのタイム・バランス
Validity Period	正式認可の絶対時間タイプの有効期限。No limitは時間無制限
Trial Validity Period	一時認可の絶対時間タイプの有効期限。No limitは時間無制限

フィールド	説明
Current State	License現在の状態の値は次のとおりです。 ● In use:現在Licenseが使用されています ● Usable:現在Licenseは使用を待機しています(デバイスに複数の相対時間Licenseが同時にインストールされており、複数のLicenseが機能をサポートしている場合、1つのLicenseの機能のみがIn useの状態になり、他のLicenseの機能はUsableの状態になります。絶対時刻License。このステータスは、有効な時刻に達していないことを示します。) ● Expired:現在のLicenseは期限切れです ● Uninstalled:現在Licenseはアンインストールされています ● Unusable:現在Licenseは使用できません Invalid:不正なデータ、使用不可
Uninstall Key	アンロードコード
Uninstall Date	アンロード日

1.1.2 display license device-id

Syntax

display license device-id

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display license device-id コマンドは、SN および DID 情報を表示するために使用します。

License アクティブ化ファイルを生成するには、アクティブ化ファイルとデバイスのバインド関係を表す DID と SN が必要です。

DID は、**license compress** コマンドの実行時に変更されます。したがって、アクティベーションファイルをリクエストする前に、デバイスの DID 情報を照会してください。

例

デバイスの SN および DID 情報を表示します。

<AC> display license device-id

```
SN:210235 A1LFX176000002
Device ID:flash:/license/210235A2G1B205000027.did
```

表 1-2 コマンド出力

フィールド	説明
SN	シリアル番号情報
Device ID	要求のデバイス番号情報License

1.1.3 display license feature

Syntax

display license feature

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display license feature コマンドで、ライセンスのサマリー情報を表示します。

例

#ライセンスのサマリー情報を表示します。

<AC> display license feature

```
Total:360Usage:1
FeatureLicensedState
APMGRN-
IOTNODEN-
```

IOTPLATN

表 1-3 コマンド出力

フィールド	説明
Total	デバイスにインストール可能なLicenseの合計数

フィールド	説明
Usage	デバイスにインストールされているLicenseの合計数
Feature	Licenseライセンスが必要なビジネス機能の名前 デバイスはEVI機能を一時的にサポートしていません
Licensed	承認済みかどうか ● Nは不正 Yは許可されていることを示します
State	Licenseの現在のステータス: ● Formalは、この機能の正式なLicenseが現在インストールされており、Licenseが有効であることを示します。 ● Trialは、この機能の一時的なLicenseが現在インストールされており、Licenseが有効であることを示します。 -現在有効なLicenseがないことを示します。この機能を使用するには、対応するLicenseをインストールしてください。

1.1.4 license activation-file install

Syntax

license activation-file install *file-name*

デフォルト

ライセンス無し

View

system view

定義済みユーザロール

network-admin

パラメータ

file-name :単一のアクティブなファイルまたはアクティブなパッケージへのフルパス。1~127 文字の文字列で、大文字と小文字が区別されます。アクティベーションファイルは、正当で有効であり、デバイスのストレージメディアに保存されている必要があります。

説明

license activation-file install コマンドを使用して、アクティブファイルをインストールします。

アクティブファイルには、次の 2 つのパブリケーション形式があります。

- ak ファイルとして独立してパブリッシュされます。ユーザは、ライセンスサーバにログインする前に認証コードを購入する必要があります。認証コードを 1 つ入力し、SN や DID などのその他の必要な情報を入力すると、拡張子が.ak のアクティベーションファイルを取得できます。
- 複数のアクティブなファイルを.tar のアクティブなパッケージとしてパブリッシュします。ライセンスサーバにログインする前に、複数の認証コードを購入する必要があります。複数の認証コードを入力し、SN や DID などのその他の必要な情報を入力すると、拡張子が.tar のアクティベーションパッケージを取得できます。このアクティブパッケージは、これらの認証コードに対応する.ak ファイルのコレクションです。アクティベーションパッケージのインストールプロセスは単一のアクティベーションファイルと同じですが、アクティベーションパッケージを使用すると、アクティベーションファイルの要求とインストールの回数が減り、アクティベーションファイルの管理が簡単になります。License をアンインストールすると、1 つのアクティブファイルのみをアンインストールできます。

ユーザは、デバイスの SN および DID を使用して、デバイスのアクティベーションファイルをリクエストする必要があります。

例

#アクティベーションファイル 20130810.ak をインストールします。

<AC> system-view

[AC] domain test

[AC-isp-test] accounting login local

ログインユーザの ISP ドメイン test のアカウンティング方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AC> system-view

[AC] license activation-file install flash:/license/20130810.ak

```
This operation might take some time.Do not perform any other operations until the
operation is completed or a failure message is displayed.Please wait ...
```

#アクティベーションパッケージ 20170101.tar をインストールします。

<AC> system-view

[AC] license activation-file install flash:/license/20170101.tar

```
This operation might take some time.Do not perform any other operations until the
operation is completed or a failure message is displayed.Please wait ...
Decompress ...... Done.
Begain to install test 01.ak ... Done.
Begain to install test 02.ak ... Done.
Begain to install test 03.ak ... Done.

Total Num:3
```

```
Success Num:3
Failed Num:0
```

関連コマンド

- display license
- display license device-id
- license activation-file uninstall

1.1.5 license activation-file uninstall

Syntax

license activation-file uninstall *file-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

file-name :単一のアクティブなファイルまたはアクティブなパッケージへのフルパス。1~127 文字の文字列で、大文字と小文字が区別されます。

説明

license activation-file uninstall コマンドは、アクティブなファイルをアンロードします。

ユーザが購入した正式なアクティベーションファイルの有効期限が切れておらず、現在のデバイスを使用する必要がない場合は、アクティベーションファイルをアンロードできます。この場合、デバイスはアンロードの認証情報であるアンロードファイルを生成します。アンインストール認証情報を他のデバイスにバインドし、新しいアクティベーションファイルを取得して新しいデバイスにインストールすることで、License を現在のデバイスから他のデバイスに移行できます。

アクティブファイルがアンロードされると、対応するプロパティはアンロードされたアクティブファイルの情報を取得できず、プロパティは実行できません。

一時アクティブ化ファイルは移行できないため、一時アクティブ化ファイルをアンロードしてもアンロードファイルは生成されません。正式にアクティブ化されたファイルをアンロードすると、アンロードファイルが生成されます

例

#アクティベーションファイル flash:/license/20130810.ak をアンインストールします。

<AC> system-view

[AC] license activation-file uninstall flash:/license/20130810.ak

```
This operation might take some time.Do not perform any other operations until the
operation is completed or a failure message is displayed.Please wait ...
Uninstall file:flash:/license/20130810.uak
```

関連コマンド

- display license
- license activation-file install

1.1.6 license compress

Syntax

license compress

View

System view

定義済みユーザロール

network-admin

パラメータ

max-times *max-times*: 各ユーザが連続してアカウンティングの更新に失敗可能な最大数を指定します。設定範囲は 1～255 です。デフォルトは 1 です。

offline: アカウンティングの更新に失敗したとき、ユーザをログオフします。

online: アカウンティングの更新に失敗したとき、ユーザをオンラインの状態で保持します。

説明

license compress コマンドは、ライセンスバケットをクリーンアップするために使用します。

License バケットスペースには制限があります。このコマンドを実行すると、デバイスはアンインストールされた承認と期限切れの承認の情報を License バケットから自動的に削除して、License バケットを解放します。

License バケットをクリーンアップすると、デバイスの DID/デバイス情報ファイルが変更される場合があります。DID/デバイス情報ファイルの変更により、既存の DID/デバイス情報ファイルを使用して要求されたが、まだインストールされていないアクティベーションファイルが後でインストールできなくなるのを防ぐため、License バケットをクリーンアップする前に、既存の DID/デバイス情報ファイルを使用して要求されたアクティベーションファイルがすべてインストールされたことを確認することをお勧めします。

例

License バケットをクリーンアップします。

<AC> system-view

[AC] license compress

```
This command will delete all data relevant to uninstalled and expired keys/licenses、
including Uninstall keys、and create a new device ID for activation keys/files.Make
sure you have saved the Uninstall keys so you can apply for a new activation key/file
for the unexpired licenses that were covered by the uninstalled activation
keys/files.
Are you sure you want to continue?[Y/N]:Y
This operation might take some time.Do not perform any other operations until the
operation is completed or a failure message is displayed.Please wait ...
```

目次

このセクションのページは **1-x-x** です。

2 章 AP ライセンス共有 2-1
2.1 AP ライセンス共有設定コマンド 2-1
2.1.1 ap-license-synchronization enable 2-1
2.1.2 display wlan ap-license-group 2-2
2.1.3 local ip 2-3
2.1.4 member ip 2-4
2.1.5 wlan ap-license-group 2-5

2章 AP ライセンス共有

2.1 APライセンス共有設定コマンド

2.1.1 ap-license-synchronization enable

Syntax

ap-license-synchronization enable

undo ap-license-synchronization enable

View

AP ライセンス共有グループビュー

定義済みユーザロール

network-admin

説明

ap-license-synchronization enable コマンドは、AP ライセンス共有を有効にします。

undo ap-license-synchronization enable コマンドは、AP ライセンス共有機能をオフにするために使用します。

AP ライセンス共有機能をオンにすると、AC はこの AC の IP アドレスを使用して AP ライセンス共有グループ内の他のメンバーAC と接続し、AP ライセンス情報を同期します。

AP ライセンス共有機能は、本 AC の IP アドレスとメンバーAC の IP アドレスが設定されている場合のみ有効です。

- デュアルリンクバックアップグループネットワークでは、両方の AC がプライマリ AC として構成されます。

N+1 コールドバックアップグループネットでは、1 台の AC のみがバックアップ AC として構成され、最大 4 台の AC がプライマリ AC として構成されます。

例

#AP ライセンス共有を有効にします。

<Switch> system-view

[Switchlan ap-license-group

[Switch-wlan-ap-license-group] ap-license-synchronization enable

2.1.2 display wlan ap-license-group

Syntax

display wlan ap-license-group

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap-license-group コマンドは、AP ライセンス共有グループの情報を表示するために使用します。

例

#AP ライセンス共有グループの情報を表示します。

<Switch> display wlan ap-license-group

```
Group total licenses:256
Group used licenses:128
AP license synchronization:Enabled
Local IP:2.2.2.2
Local role:Master
Member information:
IP address      Total    Used   Member role   State   Online duration
 2.2.2.3        128      64     Master        Up      00hr 00min 04sec
 2.2.2.4        128      64     Backup        Up      00hr 00min 09sec
 2.2.2.5        N/A      N/A    Master        Down    00hr 00min 00sec
 2.2.2.6        N/A      N/A    Master        Down    00hr 00min 00sec
```

表 2-1 コマンド出力

フィールド	説明
Group total licenses	AP license共有グループ内の合計license数
Group used licenses	AP license共有グループ内で使用されたlicenseの数
AP license synchronization	AP license共有機能の状態: ● Enabled:オン Disabled:閉じる
Local IP	本ACのIPアドレス

フィールド	説明
Local role	このACの役割: ● Master:プライマリAC ● Backup:予備AC Not configured
IP address	AP license共有グループ内のデバイスのIPアドレス
Total	合計AP license数
Used	使用されたAP licenseの数
Member role	AP license共有グループ内のデバイスの役割: ● Master:プライマリAC Backup:予備AC
State	AP license共有グループの接続ステータス: ● Up:接続が確立されました Down:接続が確立されていません
Online duration	オンライン時間の累計

2.1.3 local ip

Syntax

local ip *ipv4-address* **[backup]**

undo local ip

デフォルト

AP license 共有グループのこの AC の IP アドレスと役割が設定されていません。

View

AP ライセンス共有グループ view

定義済みユーザロール

network-admin

パラメータ

ipv4-address:AC が AP ライセンス共有グループに参加するときに使用する IP アドレス。

backup:バックアップ AC のための AP license 共有グループの AC の役割を規定して下さい。このパラメータを指定しない場合は、AC の役割がプライマリ AC であることを示します。

説明

local ip コマンドは、AP ライセンス共有グループ内のこの AC の IP アドレスと役割を設定します。

undo local ip コマンドを使用して、AP ライセンス共有グループ内のこの AC の IP アドレスと役割を削除します。

このコマンドは、AP license 共有機能がオフの場合にのみ設定できます。

例

AP ライセンス共有グループの IP アドレスを 192.168.10.10 で、役割 AC に設定します。

<Switch> system-view

[Switch] wlan ap-license-group

[Switch-wlan-ap-license-group] local ip 192.168.10.10 backup

2.1.4 member ip

Syntax

member ip *ipv4-address* **[backup]**

undo member ip *ipv4-address*

デフォルト

設定なし

View

AP ライセンス共有グループ view

定義済みユーザロール

network-admin

パラメータ

ipv4-address:AP ライセンスグループ内のメンバーAC の IP アドレスを 10 進ドット表記で共有します。

backup:メンバーロールは AC に対応しています。このパラメータを指定しない場合は、AC の役割がプライマリ AC であることを示します。

説明

member ip コマンドは、メンバーAC を AP ライセンス共有グループに追加するために使用します。

undo member ip コマンドは、AP license 共有グループのメンバーを削除するために使用します。

AP ライセンス共有グループには最大 4 つのメンバーAC を追加でき、バックアップ AC として指定できるのは 1 つのみです。

このコマンドは、AP license 共有機能がオフの場合にのみ設定できます。

例

#AP ライセンス共有グループメンバーAC を追加します。IP アドレスは 192.168.10.11、役割はバックアップ AC です。

<Switch> system-view

[Switch] wlan ap-license-group

[Switch -wlan-ap-license-group] member ip address 192.168.10.11 backup

2.1.5 wlan ap-license-group

Syntax

wlan ap-license-group

View

System view

定義済みユーザロール

network-admin

説明

wlan ap-license-group コマンドを使用して、AP ライセンス共有グループビューにアクセスします。

各 AC には 1 つのライセンス共有グループしか存在できません。

例

AP ライセンス共有グループビューに移動します。

<Switch> system-view

[Switch] wlan ap-license-group

[Switch-wlan-ap-license-group]

QX-W2300 AC シリーズ アクセスコントローラ

コマンドマニュアル

2. 基本機能

本マニュアルは以下に示す章で構成されています。

01-CLI

02-RBAC

03-ログイン管理

04- FTP

05-TFTP

06-ファイルシステム管理

07-コンフィグレーションファイル管理

08-ソフトウェアアップグレード

09- Python

10-Tcl

目次

このセクションのページは **2-x-x** です。

1 章 CLI コマンド 1-1
1.1 CLI コマンド 1-1
1.1.1 alias 1-1
1.1.2 display [| [by-linenum] { begin | exclude | include }] 1-3
1.1.3 display > 1-5
1.1.4 display >> 1-6
1.1.5 display alias 1-7
1.1.6 display history-command 1-8
1.1.7 display history-command all 1-9
1.1.8 display hotkey 1-10
1.1.9 hotkey 1-12
1.1.10 quit 1-15
1.1.11 repeat 1-16
1.1.12 return 1-17
1.1.13 screen-length disable 1-18
1.1.14 system-view 1-19

1章 CLI コマンド

1.1 CLIコマンド

1.1.1 alias

Syntax

alias *alias command*

undo alias *alias*

デフォルト

表 1-1 に示すように、一部の一般的なコマンドにはデフォルトのエイリアスが定義されています。

表 1-1 システム定義の別名

デフォルトのエイリアス	コマンド
access-list	acl
end	return
erase	delete
exit	quit
hostname	sysname
logging	info-center
no	undo
show	display
write	save

View

System view

定義済みユーザロール

network-admin

パラメータ

alias:コマンドのエイリアスを示す 1~20 文字の文字列で、大文字と小文字が区別されます。エイリアスに「alias」を使用したり、スペースを含めることはできません。

command:エイリアスを設定するコマンドで、任意の文字列を指定できます。コマンド文字列がデバイスで認識されて実行されることをユーザに確認してください。そうしないと、エイリアスコマンドの実行に失敗します。

説明

alias コマンドは、コマンドまたはコマンド文字列のエイリアスを設定するために使用します。

undo alias コマンドを使用して、適切な設定を解除します。

システム定義のデフォルトのエイリアスはキャンセルできません。

このコマンドを使用すると、コマンドラインに 1 つ以上の別名を指定したり、コマンドラインの先頭にある 1 つ以上のキーワードに複数の別名を設定したりできます。

このコマンドは、コマンドラインにエイリアスを設定し、コマンドを実行するときにエイリアスを直接使用して入力を簡略化します。たとえば、コマンド display ip routing-table のエイリアスを shiprt に設定し、display ip routing-table を使用してデバイスで有効な設定を表示する必要がある場合は、shiprt と直接入力します。

このコマンドは、コマンドラインの先頭にある 1 つ以上のキーワードにエイリアスを設定して、ユーザの習慣に合わせます。このキーワードで始まるすべてのコマンドラインは、エイリアスコマンドを使用して実行できます。たとえば、**display ip** コマンドに定義されているエイリアスは ship であり、display ip キーワードで始まるすべてのコマンドラインを使用するように ship を使用して構成できます。例:

- コマンド **display ip routing-table** を実行するには、ship routing-table と入力します。
- コマンド **display ip interface** を実行するには、ship interface と入力します。

エイリアスを設定する場合は、コマンドラインでパラメータまたはキーワードを$n で指定することができます。これにより、キーワードの一部をエイリアスに置き換えて入力を簡略化したり、必要に応じて異なるパラメータまたはキーワードを指定したりでき、柔軟性が高まります。$n は最大 9 回使用できます。n は 1~9 の整数で、引数またはキーワードの出現順を示します。たとえば、コマンド display ip $1|include $2 のエイリアスを shinc に設定した後、display ip routing-table |include Static コマンドを実行して、ルーティングテーブル内のすべての静的ルート情報をフィルタして表示する必要がある場合は、shinc routing-table Static を直接実行します。また、display ip interface |include GigabitEthernet1/0/1 を実行する必要がある場合は、shinc interface GigabitEthernet1/0/1 を直接実行できます。

例

#設定コマンド display ip routing-table のエイリアスは shiprt です。

<Sysname> system-view

[Sysname] alias shiprt display ip routing-table

[Sysname] shiprt

```
Destinations : 13       Routes : 13
Destination/Mask   Proto   Pre Cost       NextHop         Interface
```

```
0.0.0.0/32        Direct  0   0         127.0.0.1      InLoop0
3.3.3.3/32        Static  60  0         192.168.1.62    Vlan1
127.0.0.0/8       Direct  0   0         127.0.0.1      InLoop0
127.0.0.0/32      Direct  0   0         127.0.0.1      InLoop0
127.0.0.1/32      Direct  0   0         127.0.0.1      InLoop0
127.255.255.255/32 Direct  0   0         127.0.0.1      InLoop0
169.254.0.0/24    Direct  0   0         169.254.0.188   Vlan1
169.254.0.0/32    Direct  0   0         169.254.0.188   Vlan1
169.254.0.188/32   Direct  0   0         127.0.0.1      InLoop0
169.254.0.255/32   Direct  0   0         169.254.0.188   Vlan1
224.0.0.0/4       Direct  0   0         0.0.0.0        NULL0
224.0.0.0/24      Direct  0   0         0.0.0.0        NULL0
255.255.255.255/32 Direct  0   0         127.0.0.1      InLoop0
```

#設定コマンド display ip $1|include $2 のエイリアスは shinc で、エイリアスコマンドを使用して、ルーティングテーブル内のすべてのスタティックルート情報をフィルタリングして表示します。

[Sysname] alias shinc display ip $1 | include $2

#すべてのスタティックルートを表示するには、alias shinc を使用します。

[Sysname] shinc routing-table Static

```
3.3.3.3/32        Static  60  0         192.168.1.62    Vlan1
```

関連コマンド

- **display alias**

1.1.2 display [| [by-linenum] { begin | exclude | include }]

Syntax

display *command* [**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression]&<1-128>*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command:コマンドキーワード、入力して値を取得できますか?となります。

[\[by-linenum] {begin |exclude |include } regular-expression]&<1-128>:情報を表示するフィルタ規則を指定します。ここで、

- by-linenum:行番号付きで表示されます。正規表現を複数回使用して表示情報をフィルタする場合、by-linenum パラメータは 1 回の入力で有効になります。このパラメータを指定しない場合は、行番号なしで表示されます。
- begin:正規表現を含む行から表示します。
- exclude:正規表現を含まない行のみを表示します。
- include:正規表現を含む行のみを表示します。
- regular-expression:正規表現を表す 1~256 文字の文字列で、大文字と小文字が区別されます。
- &<1-128>:前のパラメータが最大 128 回入力できることを示します。

説明

display [|[by-linenum] {begin |exclude |include }]コマンドは、正規表現を使用して表示情報をフィルタするために使用します。

display コマンドを使用して表示情報を表示すると、正規表現を使用して表示情報をフィルタしたり、行番号を付けたりすることで、対象の情報をすばやく見つけることができます。正規表現の詳細については、QX-W2300 AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*1 章 CLI*”を参照してください。

複数のフィルタ条件を入力すると、すべての条件を満たす情報が表示されます。

行番号は 5 文字で、通常は行番号の後に「:」が続きます。by-linenum パラメータと begin パラメータを一緒に使用すると、行番号の後に「-」が続く場合があります。ここで、「:」はその行が照合ルールに一致することを示し、 「-」 はその行が照合ルールに一致しないことを示します。

例

#VLAN を含む設定を表示します。

<Sysname> display current-configuration |include vlan

```
vlan 1
vlan 999
port access vlan 999
```

#ログバッファに SHELL 文字列が含まれ、VTY 文字列が含まれているログを表示します。

<Sysname> display logbuffer |include SEHLL |include VTY

```
%Feb6 10:38:12:320 2020 Sysname SHELL/5/SHELL_LOGIN:VTY logged in from
169.254.100.171.
%Feb6 10:52:32:576 2020 Sysname SHELL/5/SHELL_LOGOUT:VTY logged out from
169.254.100.171.
```

```
%Feb6 16:03:27:100 2020 Sysname SHELL/5/SHELL_LOGIN:VTY logged in from
169.254.100.171.
%Feb6 16:44:18:113 2020 Sysname SHELL/5/SHELL_LOGOUT:VTY logged out from
169.254.100.171.
```

#現在の構成を表示します。「user-group」文字列を含む行から最後の行まで構成情報が表示され、行番号も表示されます。(行番号の後に 「:」 が付いている場合は、その行に「user-group」文字列が含まれていることを示し、 「-」 が付いている場合は、その行に「user-group」文字列が含まれていないことを示します。)

<Sysname> display current-configuration |by-linenum begin user-group

```
114:user-group system
115-#
116-return
```

1.1.3 display >

Syntax

display *command >filename*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command:コマンドキーワード、入力して値を取得できますか?となります。

filename:ファイル名。1~63 文字の文字列です。

説明

display >コマンドを使用すると、表示情報を個別にファイルに保存できます。

display コマンドで表示される内容は、通常、統計情報、機能が有効かどうか、および機能に関連するパラメータ設定です。これらの情報は、デバイスの実行中やユーザの設定によって変わります。このコマンドを使用して、現在表示されている情報をファイルに保存し、いつでも比較して表示できます。

このコマンドを実行すると、filename が存在しない場合は、保存する前にファイルが作成されます。filename がすでに存在する場合は、元のファイルの内容が上書きされます。

例

#display vlan 1 の表示情報を vlan.txt ファイルに保存します。

<Sysname> display vlan 1 >vlan.txt

vlan.txt の内容を確認し、display >コマンドの実行結果を確認します。

<Sysname> more vlan.txt

```
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/2
```

1.1.4 display >>

Syntax

display *command* **>>***filename*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command:コマンドキーワード、入力して値を取得できますか?となります。

filename:ファイル名。1~63 文字の文字列です。

説明

display >>コマンドは、表示情報をファイルに追加で保存します。

display コマンドで表示される内容は、通常、統計情報、機能が有効かどうか、および機能に関連するパラメータ設定です。これらの情報は、デバイスの実行中やユーザの設定によって変わります。このコマンドを使用して、現在表示されている情報をファイルに保存し、いつでも比較して表示できます。

このコマンドを実行すると、filename が存在しない場合は、ファイルが保存される前に作成されます。filename がすでに存在する場合は、新しく保存された内容が filename ファイルの末尾に追加されます。

例

#display vlan 999 の表示情報をファイル vlan.txt に追加保存する。

<Sysname> display vlan 999 >>vlan.txt

vlan.txt の内容を確認し、display >>コマンドの実行結果を確認します。

<Sysname> more vlan.txt

```
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:  None
 Untagged ports:
   GigabitEthernet1/0/2

 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:  None
 Untagged ports:
   GigabitEthernet1/0/2
```

1.1.5 display alias

Syntax

display alias [*alias*]

View

すべてのビュー

定義済みユーザロール

network-admin

network-operator

パラメータ

alias:設定されたコマンドエイリアスを表します。このパラメータを指定しないと、構成済みのコマンドエイリアスがすべて表示されます。

例

#システムで構成されているすべてのコマンドエイリアスを表示します。

<Sysname> display alias

```
Index     Alias              Command key
1         logging            info-center
2         show               display
3         shinc              display ip $1 | include $2
4         erase              delete
5         access-list         acl
6         no                 undo
7         exit               quit
8         end                return
9         hostname           sysname
10        write              save
```

#エイリアスコマンド shinc が表すコマンド文字列を表示します。

<Sysname> display alias shinc

```
Alias              Command key
shinc              display ip $1 | include $2
```

表 1-2 display alias コマンドの表示情報の説明

フィールド	説明する
Index	インデックス番号
Alias	別名
Command key	コマンド文字列

説明

display alias コマンドを使用して、コマンドエイリアスの関連する設定を表示します。

関連コマンド

- **alias**

1.1.6 display history-command

Syntax

display history-command

View

全てのビュー

定義済みユーザロール

network-admin

network-operator

説明

display history-command コマンドは、現在のログインユーザ履歴コマンドバッファ内のコマンドを表示します。

ユーザがデバイスにログインすると、各ユーザには履歴コマンドバッファが自動的に割り当てられます。履歴コマンドバッファには、ユーザがログインしたときに正常に実行されたコマンドラインが格納され、ユーザが表示して呼び出すことができます。ヒストリカル・コマンド・キャッシュにはサイズ制限があり、デフォルトで 10 個のコマンドが保存されます。**history-command max-size** コマンドを使用してサイズを変更することもできます。最大数に達すると、最も古いレコードが自動的に削除され、最後に正常に実行されたコマンドが保存されます。

ユーザがログインを終了すると、履歴コマンド・キャッシュ・エリアのすべてのレコードが自動的に消去されます。

パスワード構成コマンドが履歴コマンドバッファに存在する場合、デバイスのセキュリティを向上させるために、パスワードは******と表示されます。

例

#履歴コマンドキャッシュに保存されているコマンドを表示します。

<Sysname> display history-command

system-view

vlan 2

quit

1.1.7　display history-command all

Syntax

display history-command all

View

全てのビュー

定義済みユーザロール

network-admin

説明

display history-command all コマンドは、すべてのログインユーザ履歴コマンドバッファ内のコマンドを表示します。

システムには、ログインしているすべてのユーザが正常に実行したコマンドラインを保持する共有履歴コマンドバッファがあり、ユーザは(呼び出すことができません)を参照できます。履歴コマンドキャッシュ領域のサイズは 1024 に固定されており、設定できませ

ん。最大数に達すると、最も古いレコードが自動的に削除され、最後に正常に実行されたコマンドが保存されます。

ユーザがログインを終了しても、共有履歴コマンドキャッシュ内のそのユーザの履歴コマンド・レコードは消去されません。

パスワード構成コマンドが履歴コマンドバッファに存在する場合、デバイスのセキュリティを向上させるために、パスワードは******と表示されます。

例

#すべてのログインユーザが正常に実行した履歴コマンドを表示します。

<Sysname> display history-command all

```
日付 TimeTerminalIp ユーザ
02/16/2020 20:03:33 vty 0192.168.1.26**
Cmd:dis his all

02/16/2020 20:03:29 vty 0192.168.1.26**
Cmd:sys
```

表 1-3 display history-command all コマンドの表示情報の説明

フィールド	説明
Date	コマンドラインを実行した日付
Time	コマンドラインの実行時間
Terminal	コマンドを実行するユーザが使用するログインユーザ線
Ip	コマンドを実行するユーザが使用するログインIP
User	ユーザがデバイスにschemeでログインした場合、このフィールドには、コマンドを実行したユーザが使用したログインユーザ名が表示されます。別の方法でデバイスにログインした場合、このフィールドには**と表示されます。
Cmd	実行されるコマンド(ユーザの入力との整合性)

関連コマンド

- display history-command

1.1.8 display hotkey

Syntax

display hotkey

View

全てのビュー

定義済みユーザロール

network-admin

network-operator

説明

display hotkey コマンドは、システムでサポートされているショートカットとその意味を表示します。

例

#システムでサポートされているショートカットとその意味を表示します。

<Sysname> display hotkey

```
----------------- Hotkeys -----------------

         -Defined function hotkeys-
CTRL_A  Move the cursor to the beginning of the line.
CTRL_B  Move the cursor one character to the left.
CTRL_C  Stop the current command.
CTRL_D  Erase the character at the cursor.
CTRL_E  Move the cursor to the end of the line.
CTRL_F  Move the cursor one character to the right.
CTRL_H  Erase the character to the left of the cursor.
CTRL_K  Abort the connection request.
CTRL_N  Display the next command in the history buffer.
CTRL_P  Display the previous command in the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word to the left of the cursor.
CTRL_X  Delete all characters from the beginning of the line to the cursor.
CTRL_Y  Delete all characters from the cursor to the end of the line.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor back one word.
ESC_D   Delete all characters from the cursor to the end of the word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Move the cursor to the beginning of the clipboard.
ESC_>   Move the cursor to the end of the clipboard.

         -Defined command hotkeys-
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
```

```
CTRL_O  undo debugging all

          -Undefined hotkeys-
CTRL_T  NULL
CTRL_U  NULL
```

表 1-4 display hotkey コマンドの表示情報の説明

フィールド	説明
Defined function hotkeys	定義されたバインド機能のショートカットキー
Defined command hotkeys	定義済みのバインドコマンドのショートカットキー
Undefined hotkeys	定義されていないショートカット

各キーバインドの機能やコマンドの詳細については、表 1-5 を参照してください。

関連コマンド

- **hotkey**

1.1.9 hotkey

Syntax

hotkey *hotkey {command* |**function** *function* **|none }**

undo hotkey *hotkey*

デフォルト

デバイスは 29 個のショートカットをサポートしています。各ショートカットのデフォルトのバインド関係は表 1-5 のとおりです。

表 1-5 ショートカットのデフォルトの結合関係

ショートカットキー	デフォルト・バインディングの機能またはコマンド
CTRL_A	**move_the_cursor_to_the_beginning_of_the_line**は、カーソルを現在の行の先頭に移動します。
CTRL_B	**move_the_cursor_one_character_to_the_left:**カーソルを左に1文字移動します。
CTRL_C	**stop_the_current_command**。現在実行中の機能を停止します。
CTRL_D	**erase_the_character_at_the_cursor**現在のカーソル位置の文字を削除する
CTRL_E	**move_the_cursor_to_the_end_of_the_line**は、カーソルを現在の行の最後に移動します。
CTRL_F	**move_the_cursor_one_character_to_the_right**は、カーソルを1文字右に移

ショートカットキー	デフォルト・バインディングの機能またはコマンド
	動します。
CTRL_G	**display current-configuration**:現在の構成を表示します。
CTRL_H	**erase_the_character_to_the_left_of_the_cursor**カーソルの左側にある1文字を削除する
CTRL_K	**abort_the_connection_request**は、アウトバウンド接続の終了を示します。
CTRL_L	**display ip routing-table**は、IPv 4ルーティングテーブル情報を表示します。
CTRL_N	**display_the_next_command_in_the_history_buffer**履歴バッファ内の次のコマンドを表示する(パスワード構成コマンドがスキップされる)
CTRL_O	**undo debugging all**は、すべての機能項目のデバッグ・スイッチをオフにします。
CTRL_P	**display_the_previous_command_in_the_history_buffer**履歴バッファ内の最後のコマンドを表示する(パスワード構成コマンドがスキップされる)
CTRL_R	**redisplay_the_current_line**:現在の明細情報を再表示します。
CTRL_T	コマンドラインまたは機能がバインドされていません
CTRL_U	コマンドラインまたは機能がバインドされていません
CTRL_V	**paste_text_from_the_clipboard**クリップボードの内容を貼り付ける
CTRL_W	**delete_the_word_to_the_left_of_the_cursor**は、カーソルの左側にある連続する文字列内のすべての文字を削除することを意味します。
CTRL_X	**delete_all_characters_from_the_beginning_of_the_line_to_the_cursor**カーソルの左側にあるすべての文字を削除する
CTRL_Y	**delete_all_characters_from_the_cursor_to_the_end_of_the_line**は、カーソル位置とその右側にあるすべての文字を削除することを意味します。
CTRL_Z	**return_to_the_User_View**は、ユーザビューに戻ることを示します。
CTRL_]	現在の接続を終了するには、**kill_incoming_connection_or_redirect_connection**
ESC_B	**move_the_cursor_back_one_word**:カーソルを左側の連続する文字列の先頭に移動します。
ESC_D	**delete_all_characters_from_the_cursor_to_the_end_of_the_word**は、カーソル位置とその右側の連続する文字列内のすべての文字を削除することを意味します。
ESC_F	**move_the_cursor_forward_one_word**:次の連続する文字列の前にカーソルを右に移動します。
ESC_N	**move_the_cursor_down_a_line**は、カーソルを1行下に移動することを示します(入力キャリッジリターン前に有効)。
ESC_P	**move_the_cursor_up_a_line**:カーソルを1行上に移動します(入力キャリッジリターン前に有効)。
ESC_<	**move_the_cursor_to_the_beginning_of_the_clipboard**は、カーソルの位置をクリップボードの開始位置として指定します。
ESC_>	**move_the_cursor_to_the_end_of_the_clipboard**は、カーソルの位置をクリ

ショートカットキー	デフォルト・バインディングの機能またはコマンド
	ップボードの終了位置として指定します。

View

System view

定義済みユーザロール

network-admin

パラメータ

hotkey:バインドするショートカットが必要です。デバイスでサポートされているショートカットである必要があります。値については、表 1-5 を参照するか、hotkey を実行してください。コマンドを使用して、パラメータの値を指定できます。

command:ショートカットキーのバインドのコマンドライン。デバイスで正常に実行できるコマンドラインである必要があります。

function *function*:ショートカットバインディングの機能。hotkey hotkey function を実行しますか?コマンドは、このパラメータの値の取得に役立ちます。各値の意味については、表 1-5 を参照してください。

none:ショートカットのバインド関係を指定解除します。このパラメータを設定すると、ショートカットはコマンドや機能にバインドされません。

説明

hotkey コマンドを使用して、ショートカットのバインド関係を変更します。

undo hotkey コマンドを使用して、デフォルトの状態を復元します。

ユーザがデバイスを操作しやすくするため、デバイスは 29 個のショートカットをサポートし、ユーザは「CTRL_]」を除く 28 個のショートカットの結合関係を変更できる。ユーザがショートカットキーを押すと、デバイスは対応するコマンドラインまたは機能を実行します。これらのショートカットがユーザのログイン端末で定義されたショートカットと競合したり、ユーザの使用習慣に合わない場合、ユーザはこのコマンドを使用してショートカットを再定義したり、ショートカットのバインド関係を解除したりできます。

1 つのショートカットは 1 つのコマンドまたは機能に対応します。このコマンドを使用して同じショートカットを複数回定義すると、最新の設定が有効になります。このコマンドを複数回使用して、同じコマンドや機能に複数のショートカットをバインドした場合は、そのショートカットが有効になります。

ユーザが端末ソフトウェアを使用してデバイスと対話する場合、端末ソフトウェアがショートカットを定義すると(ユーザ定義およびシステム定義のショートカットを含む)、ショートカットは端末ソフトウェアの定義に従います。

例

#ショートカット<Ctrl+U>と機能「カーソルを現在の行の先頭に移動」をバインドします。

<Sysname> system-view

[Sysname] hotkey ctrl_u function move_the_cursor_to_the_beginning_of_the_line

#ショートカット<Ctrl+A>のバインドを解除します。

<Sysname> system-view

[Sysname] hotkey ctrl_a none

関連コマンド

- display hotkey

1.1.10 quit

Syntax

quit

View

すべてのビュー

定義済みユーザロール

network-admin

network-operator

説明

quit コマンドは、ユーザを現在のビューから前のビューに戻すために使用します。

現在ユーザビューの場合、quit を実行すると、現在の接続が切断され、システムが終了します。

例

#インタフェース GigabitEthernet1/0/1 ビューからシステムビューに戻り、ユーザビューに戻ります。

[Sysname-GigabitEthernet1/0/1] quit

[Sysname] quit

<Sysname>

1.1.11 repeat

Syntax

repeat [*number*] [**count** *times*] [**delay** *seconds*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

number: 現在の CLI セッションのコマンド履歴バッファで、繰り返し実行したい直近のコマンド数を指定します。値の範囲は 1～256 です。デフォルトは 1 です。

count *times*: コマンドを実行する回数を指定します。値の範囲は 0～4294967295 です。デフォルトは 0 です。このオプションを指定しない場合、エスケープキーを押して停止するまで実行は継続されます。

delay *seconds*: コマンドを再実行する前にシステムが待機する時間（秒）を指定します。値の範囲は 0～4294967295 です。デフォルトは 1 です。

説明

repeat コマンドを使用すると、現在の CLI セッションのコマンド履歴バッファ内のコマンドを繰り返し実行できます。

コマンドを繰り返す場合、まずそのコマンドのビューに入ります。複数のコマンドを繰り返す場合は、最初のコマンドのビューに入ります。

対話型コマンドを繰り返す際、システムはユーザの操作を待機します。

パスワード設定コマンドはすべてスキップされます。

コマンド履歴バッファで繰り返されるコマンド数は、以下の最小値によって決まります。

· repeat コマンドで指定した直近のコマンド数

· history-command max-size コマンドで指定したコマンド履歴バッファのサイズ

· コマンド履歴バッファ内のコマンド数

例

直近に実行した 2 つのコマンド（display cpu-usage と display clock）を 10 秒間隔で 2 回実行します。

<AC> repeat 2 count 2 delay 10

```
<AC> display cpu
Unit CPU usage:
     33% in last 5 seconds
     32% in last 1 minute
```

```
     33% in last 5 minutes

<AC> display clock
07:02:18 UTC Thu 06/19/2017
<AC> display cpu-usage
Unit CPU usage:
     33% in last 5 seconds
     32% in last 1 minute
     33% in last 5 minutes

<AC> display clock
07:02:28 UTC Thu 06/19/2017
```

1.1.12 return

Syntax

return

View

Tcl 構成ビューと Python shell 以外の非ユーザビュー

定義済みユーザロール

network-admin

network-operator

説明

return コマンドは、現在のビュー(Tcl 構成ビューと Python shell 以外の非ユーザビュー)からユーザビューに直接戻るために使用します。

また、キーの組み合わせ<Ctrl+Z>を使用して、現在のビュー(Tcl 構成ビューと Python shell 以外の非ユーザビュー)からユーザビューに直接戻ることもできます。これは、return コマンドを実行した場合と同じです。

Tcl 設定ビューおよび Python shell はそれぞれ次のようにユーザビューにロールバックされます。

- Tcl 設定ビューの下でユーザビューに戻るのに tclquit を使用して下さい。
- Python shell で exit ()コマンドを実行して、Python shell からユーザビューに戻ります。

例

#インタフェース GigabitEthernet1/0/1 ビューからユーザビューに戻ります。

[Sysname-GigabitEthernet1/0/1] return

<Sysname>

1.1.13 screen-length disable

Syntax

screen-length disable

undo screen-length disable

デフォルト

デフォルトは、ユーザラインビューの screen-length コマンドの設定に依存します。

screen-length コマンドのデフォルト設定は次のとおりです。

- 出力画面間の一時停止。
- 画面に最大 24 行表示する。

View

ユーザビュー

定義済みユーザロール

network-admin

説明

screen-length disable コマンドは、現在のユーザの分割画面表示をオフにします。

undo screen-length disable コマンドは、現在のユーザの分割画面表示をオンにします。

情報収集時は分割画面表示機能をオフにすることをお勧めします。分割画面表示機能をオフにすると、一度にすべての情報が表示されます。情報を見る時に、分割画面表示機能をオフにすることはお勧めしません。情報が多いと、連続的に画面をスワイプします。すぐに見るのは不便です。

この構成は、現在のユーザがログインした場合にのみ有効です。ユーザがログインし直すと、デフォルトに戻ります。

例

#現在のユーザの分割画面表示をオフにします。

<Sysname> screen-length disable

関連コマンド

- **screen-length (基本機能-ログイン管理)**

1.1.14 system-view

Syntax

system-view

View

ユーザビュー

定義済みユーザロール

network-admin

network-operator

説明

system-view コマンドは、ユーザビューからシステムビューに移動するために使用します。

例

#ユーザビューからシステムビューに移動します。

<Sysname> system-view

```
System View: return to User View with Ctrl+Z.
```

[Sysname]

目次

このセクションのページは **2-x-x** です。

2 章 RBAC 構成コマンド 2-1
2.1 RBAC 構成コマンド 2-1
2.1.1 description 2-1
2.1.2 display role 2-2
2.1.3 display role feature 2-10
2.1.4 display role feature-group 2-12
2.1.5 feature 2-15
2.1.6 interface policy deny 2-16
2.1.7 permit interface 2-17
2.1.8 permit vlan 2-19
2.1.9 role 2-21
2.1.10 role default-role enable 2-23
2.1.11 role feature-group 2-24
2.1.12 rule 2-25
2.1.13 super 2-30
2.1.14 super authentication-mode 2-31
2.1.15 super default role 2-33
2.1.16 super password 2-34
2.1.17 vlan policy deny 2-35

2章 RBAC 構成コマンド

2.1 RBAC構成コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

ユーザロールの説明情報が定義されていません。

View

ユーザロールビュー

定義済みユーザロール

network-admin

パラメータ

text:ユーザロールの説明情報。1~128 文字の文字列で、大文字と小文字が区別されます。

説明

description コマンドは、管理者がユーザロールを管理しやすいように、ユーザロールの説明情報を設定します。

undo description コマンドを使用して、デフォルトの状態を復元します。

例

#ユーザロール role1 の設定説明情報は「labVIP」です。

<Sysname> system-view

[Sysname] role name role1

[Sysname-role-role1] description labVIP

関連コマンド

- display role
- role

2.1.2 display role

Syntax

display role [name *role-name* **]**

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

name *role-name*:ユーザロール名。1~63 文字の文字列で、大文字と小文字が区別されます。ユーザロール名を指定しない場合は、システムにデフォルトで存在するユーザロールの情報を含む、すべてのユーザロールの情報が表示されます。

説明

display role コマンドを使用して、ユーザの役割情報を表示します。

例

#ユーザロール 123 の情報を表示する。

<Sysname> display role name 123

```
Role: 123
  Description: 123
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
```

#すべてのユーザロールの情報を表示します。

<sysname> display role

```
Role: network-admin
  Description: Predefined network admin role has access to all commands on the
d
evice
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
```

```
  ------------------------------------------------------------------
  sys-1   permit      command      *
  sys-2   permit RWX   web-menu     -
  sys-3   permit RWX   xml-element   -
  sys-4   deny        command      display security-logfile summary
  sys-5   deny        command      display security-logfile buffer
  sys-6   deny        command      system-view ; info-center securi
                                 ty-logfile directory *
  sys-7   deny        command      security-logfile save
  sys-8   permit RW-   oid         1
  R:Read W:Write X:Execute

Role: network-operator
  Description: Predefined network operator role has access to all read commands
on the device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ------------------------------------------------------------------
  sys-1   permit      command      display *
  sys-2   permit      command      xml
  sys-3   permit      command      system-view ; probe ; display *
  sys-4   deny        command      display history-command all
  sys-5   deny        command      display exception *
  sys-6   deny        command      display cpu-usage configuration
                                 *
  sys-7   deny        command      display kernel exception *
  sys-8   deny        command      display kernel deadloop *
  sys-9   deny        command      display kernel starvation *
  sys-10  deny        command      display kernel reboot *
  sys-13  permit      command      system-view ; local-user *
  sys-15  permit R--   web-menu     -
  sys-16  permit R--   xml-element   -
  sys-17  permit --X   xml-element   useraccounts/changemypassword
  sys-18  permit --X   xml-element   rpc
  sys-19  deny        command      display security-logfile summary
  sys-20  deny        command      display security-logfile buffer
  sys-21  deny        command      system-view ; info-center securi
                                 ty-logfile directory *
  sys-22  deny        command      security-logfile save
```

```
  sys-23  deny       command      system-view ; local-user-import
                                  *
  sys-24  deny       command      system-view ; local-user-export
                                  *
  sys-25  permit R--   oid          1
  R:Read W:Write X:Execute

Role: level-0
  Description: Predefined level-0 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ----------------------------------------------------------------------
  sys-1   permit      command      tracert *
  sys-2   permit      command      telnet *
  sys-3   permit      command      ping *
  sys-4   permit      command      ssh2 *
  sys-5   permit      command      super *
  R:Read W:Write X:Execute

Role: level-1
  Description: Predefined level-1 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ----------------------------------------------------------------------
  sys-1   permit      command      tracert *
  sys-2   permit      command      telnet *
  sys-3   permit      command      ping *
  sys-4   permit      command      ssh2 *
  sys-5   permit      command      display *
  sys-6   permit      command      super *
  sys-7   deny        command      display history-command all
  R:Read W:Write X:Execute

Role: level-2
  Description: Predefined level-2 role
```

```
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-3
  Description: Predefined level-3 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-4
  Description: Predefined level-4 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-5
  Description: Predefined level-5 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-6
  Description: Predefined level-6 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-7
  Description: Predefined level-7 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-8
  Description: Predefined level-8 role
  VLAN policy: permit (default)
```

```
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-9
  Description: Predefined level-9 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   feature      -
  sys-2   deny   RWX   feature      device
  sys-3   deny   RWX   feature      filesystem
  sys-4   permit       command      display *
  sys-5   deny         command      display history-command all
  R:Read W:Write X:Execute

Role: level-10
  Description: Predefined level-10 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-11
  Description: Predefined level-11 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-12
  Description: Predefined level-12 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-13
  Description: Predefined level-13 role
```

```
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-14
  Description: Predefined level-14 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ------------------------------------------------------------------
  sys-1   permit      command      *
  sys-2   permit RWX   web-menu     -
  sys-3   permit RWX   xml-element   -
  sys-4   deny        command      display security-logfile summary
  sys-5   deny        command      display security-logfile buffer
  sys-6   deny        command      system-view ; info-center securi
                                  ty-logfile directory *
  sys-7   deny        command      security-logfile save
  sys-8   permit RW-   oid         1
  R:Read W:Write X:Execute

Role: security-audit
  Description: Predefined security audit role only has access to commands for th
e security log administrator
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ------------------------------------------------------------------
  sys-1   deny        command      *
```

```
  sys-2   permit      command      display security-logfile summary
  sys-3   permit      command      display security-logfile buffer
  sys-4   permit      command      system-view ; info-center securi
                                 ty-logfile directory *
  sys-5   permit      command      security-logfile save
  sys-6   permit      command      cd *
  sys-7   permit      command      copy *
  sys-8   permit      command      delete *
  sys-9   permit      command      dir *
  sys-10  permit      command      mkdir *
  sys-11  permit      command      more *
  sys-12  permit      command      move *
  sys-13  permit      command      rmdir *
  sys-14  permit      command      pwd
  sys-15  permit      command      rename *
  sys-16  permit      command      undelete *
  sys-17  permit      command      ftp *
  sys-18  permit      command      sftp *
  R:Read W:Write X:Execute

Role: guest-manager
  Description: Predefined guest manager role can't access to commands
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  Security zone policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ----------------------------------------------------------------------
  sys-1   permit RWX   xml-element   useraccounts/approveguest/
  sys-2   permit RWX   xml-element   useraccounts/exportguestaccount/
  sys-3   permit RWX   xml-element   useraccounts/generateguestaccoun
                                   t/
  sys-4   permit RWX   xml-element   useraccounts/guest/
  sys-5   permit RWX   xml-element   useraccounts/guestconfigure/
  sys-6   permit RWX   xml-element   useraccounts/importguestaccount/
  sys-7   permit RWX   xml-element   useraccounts/exportguesttemplet/
  sys-8   permit --X   xml-element   useraccounts/changemypassword
  sys-9   permit RWX   xml-element   rpc/
  sys-10  deny        command      *
  R:Read W:Write X:Execute
```

表 2-1 display role コマンドの表示情報の説明

フィールド	説明
role	ユーザロール名。システム定義のユーザロール名は、network-admin、network-operator、level-n (nは0~15)、security-audit、guest-managerです。
Description	ユーザの役割の説明
VLAN policy	設定されたVLANポリシー: • deny:操作許可で指定された VLAN 以外の VLAN はユーザが操作できないことを示す. • permit (default):システムがデフォルトで任意の VLAN の操作を許可していることを示します。
Permitted VLANs	ユーザが操作できるVLAN
Interface policy	設定されたインタフェースポリシー: • deny:許可された操作で指定されたインタフェース以外のインタフェースは､ユーザが操作できないことを示します。 • permit (default):システムでデフォルトで任意のインタフェースの操作が許可されていることを示します。
Permitted interfaces	ユーザの操作を可能にするインタフェース
VPN-instance policy	(未サポート)設定されたVPNポリシー: • deny:許可操作で指定された VPN インスタンスを除き、他の VPN インスタンスはユーザ操作できないことを示す. • permit (default):システムがデフォルトでユーザに任意の VPN インスタンスの操作を許可していることを示します。
Permitted VPN instances	(未サポート)ユーザが操作できるVPNインスタンス
Rule	ユーザロール規則番号(システム定義の権限ルールはsys-nで識別されます。)
perm	コマンドラインに対する操作の許可: • permit:操作の許可 • deny deny:操作の禁止ソウサノホジ
Type	コマンドラインのタイプ: • R:読み取りタイプ • W:書き込みタイプ • X:実行タイプ

フィールド	説明
Scope	ユーザロール規則のタイプ: ● command:コマンドラインベースの規則 ● feature:プロパティに基づく規則 ● feature-group:プロパティグループ規則に基づく ● web-menu:Webメニューベースのルール ● xml-element:XML要素に基づく規則 ● oid:OID要素に基づく規則
Entity	ユーザの役割の規則で定義されている特定の内容(コマンドフィーチャー文字列、プロパティ名、プロパティグループ名、Webメニュー、XML要素、またはOID) ● 「-」 はすべてのプロパティを表します ● 「*」 は、0個以上の任意の文字を表すワイルドカードです。

関連コマンド

- role

2.1.3 display role feature

Syntax

display role feature [name *feature-name* **|verbose]**

View

すべてのビュー

定義済みユーザロール

network-admin

network-operator

パラメータ

name *feature-name*:指定したプロパティの詳細が表示されます。feature-name はシステム内のプロパティ名を表し、すべてのプロパティ名の文字は小文字です。

verbose:すべてのプロパティの詳細を表示します。つまり、プロパティに含まれるすべてのコマンドラインのリストを表示します。

説明

display role feature コマンドを使用して、プロパティに関する情報を表示します。

キーワードを指定しない場合は、システム内のすべてのプロパティの名前のリストが表示されます。

例

#システム内のすべてのプロパティの名前のリストを表示します。

<Sysname> display role feature

```
Feature:device(Device configuration related commands)
Feature:interface(Interface related commands)
Feature:syslog(Syslog related commands)
...... (略)
```

#すべてのプロパティの詳細を表示します。

<Sysname> display role feature verbose

```
Feature:device(Device configuration related commands)
display clock(R)
debugging dev(W)
display debugging dev(R)
display device *(R)
...... (略)
```

#プロパティ aaa の詳細を表示します。

<Sysname> display role feature name aaa

```
Feature:aaa(AAA related commands)
system-view ;domain *(W)
system-view ;header *(W)
system-view ;aaa*(W)
system-view ;interface *;aaa*(W)
display domain *(R)
display max-user *(R)
display debugging aaa *(R)
debugging aaa *(W)
display aaa *(R)
reset aaa *(W)
...... (略)
```

表 2-2 display role feature コマンド情報説明表を表示する(例:display role feature name aaa の表示フィールド)

フィールド	説明
Feature	機能名と機能概要
system-view ;domain *	システムビューのdomainで始まるすべてのコマンド、およびISPドメインビューのすべてのコマンド
system-view ;header *	システムビューでheaderで始まるすべてのコマンド
system-view ;aaa*	システムビューのaaaで始まるすべてのコマンド

フィールド	説明
system-view ;interface *;aaa*	インタフェースビューのaaaで始まるすべてのコマンド
display domain *	ユーザビューでdisplay domainで始まるすべてのコマンド
display max-user *	ユーザビューでdisplay max-userで始まるすべてのコマンド
display debugging aaa *	ユーザビューでdisplay debugging aaaで始まるすべてのコマンド
debugging aaa *	ユーザビューでdebugging aaaで始まるすべてのコマンド
display aaa *	ユーザビューでdisplay aaaで始まるすべてのコマンド
reset aaa *	ユーザビューでreset aaaで始まるすべてのコマンド
(W)	コマンドラインのタイプは書き込みコマンドです。このタイプのコマンドは、システムの構成に使用されます。
(R)	コマンドラインのタイプは読み取りコマンドです。このタイプのコマンドで表示できるのは、システム構成情報とメンテナンス情報のみです。
(X)	コマンドラインのタイプは実行コマンドです。このタイプのコマンドは、特定の機能を実行するために使用されます。

関連コマンド

- feature

2.1.4 display role feature-group

Syntax

display role feature-group [name *feature-group-name* **] [verbose]**

View

すべてのビュー

定義済みユーザロール

network-admin

network-operator

パラメータ

name *feature-group-name*:指定したプロパティグループに含まれるプロパティ名のリストを表示します。feature-group-name は、プロパティグループ名を示す 1~31 文字の文字列で、大文字と小文字が区別されます。このパラメータを指定しない場合は、すべてのプロパティグループに関する情報が表示されます。

verbose:プロパティグループの詳細を表示します。プロパティグループ内のプロパティに含まれるコマンドラインのリストが表示されます。このパラメータを指定しない場合は、プロパティグループ内のプロパティ名のリストが表示されます。

定義済みユーザロール

display role feature-group コマンドは、プロパティグループ情報を表示します。

説明

機能グループ L 2 と L 3 は、システム定義済みの 2 つの機能グループです。

例

#すべてのプロパティグループ内のプロパティ名のリストを表示します。

<Sysname> display role feature-group

```
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
Feature: mld-snooping    (MLD-Snooping related commands)
Feature: lacp           (LACP related commands)
Feature: stp            (STP related commands)
Feature: lldp           (LLDP related commands)
Feature: loopbk-detect   (Loopback-detection related commands)
Feature: vlan           (Virtual LAN related commands)
Feature: port-security   (Port-security related commands)

Feature group: L3
Feature: route          (Route management related commands)
Feature: staticrt       (Unicast static route related commands)
Feature: ospf           (Open Shortest Path First protocol related commands)
Feature: rip            (Routing Information Protocol related commands)
Feature: lisp           (LISP protocol related commands)
Feature: route-policy    (Routing Policy related commands)
Feature: multicast      (Multicast related commands)
```

#すべての機能グループの詳細を表示します。

<Sysname> display role feature-group verbose

```
Feature group: L2
Feature: igmp-snooping   (IGMP-Snooping related commands)
  system-view ; igmp-snooping *    (W)
```

```
  system-view ; multicast-vlan *    (W)
  system-view ; vlan * ; igmp-snooping *    (W)
  system-view ; vlan * ; pim-snooping *    (W)
  system-view ; interface * ; igmp-snooping *    (W)
  system-view ; interface * ; port multicast-vlan *    (W)
  display igmp-snooping *    (R)
  display pim-snooping *    (R)
  display multicast-vlan *    (R)
  display l2-multicast *    (R)
  system-view ; probe ; display system internal l2-multicast *    (R)
  reset igmp-snooping *    (W)
  reset pim-snooping *    (W)
  reset multicast-vlan *    (W)
  reset l2-multicast *    (W)
  debugging igmp-snooping *    (W)
  display debugging igmp-snooping *    (R)
  system-view ; probe ; debugging system internal igmp-snooping *    (W)
Feature: mld-snooping    (MLD-Snooping related commands)
  system-view ; mld-snooping *    (W)
  system-view ; ipv6 multicast-vlan *    (W)
  system-view ; vlan * ; mld-snooping *    (W)
  system-view ; vlan * ; ipv6 pim-snooping *    (W)
  system-view ; interface * ; mld-snooping *    (W)
  system-view ; interface * ; ipv6 port multicast-vlan *    (W)
  display mld-snooping *    (R)
  display ipv6 pim-snooping *    (R)
  display ipv6 multicast-vlan *    (R)
  display ipv6 l2-multicast *    (R)
  system-view ; probe ; display system internal ipv6 l2-multicast *    (R)
  reset mld-snooping *    (W)
  reset ipv6 pim-snooping *    (W)
  reset ipv6 multicast-vlan *    (W)
  reset ipv6 l2-multicast *    (W)
  debugging mld-snooping *    (W)
...
```

#プロパティグループ L 3 のプロパティ名のリストを表示します。

<Sysname> display role feature-group name L3

```
Feature group: L3
Feature: route          (Route management related commands)
Feature: staticrt       (Unicast static route related commands)
Feature: lisp           (LISP protocol related commands)
Feature: multicast      (Multicast related commands)
```

表 2-3 display role feature-group コマンドの表示情報の説明

フィールド	説明
Feature group	プロパティグループ名。ここで、L 2とL 3はシステム定義済みの2つのプロパティグループです。
Feature	機能名と機能概要 プロパティ内の具体的なコマンドの詳細については表 2-2を参照してください。

関連コマンド

- feature
- role feature-group

2.1.5 feature

Syntax

feature *feature-name*

undo feature *feature-name*

デフォルト

カスタムプロパティグループにはプロパティは含まれません。

View

プロパティグループビュー

定義済みユーザロール

network-admin

パラメータ

feature-name: プロパティ名を指定します。プロパティ名は小文字で入力する必要があります。

説明

feature コマンドは、プロパティグループにプロパティを追加するために使用します。

undo feature コマンドは、プロパティグループから指定したプロパティを削除します。

このコマンドを複数回実行すると、プロパティグループに複数のプロパティを追加できます。

例

#機能グループ security-features に機能 AAA と ACL を追加します。

<Sysname> system-view

[Sysname] role feature-group name security-features

[Sysname-featuregrp-security-features] feature aaa

[Sysname-featuregrp-security-features] feature acl

関連コマンド

- display role feature
- display role feature-group
- role feature-group

2.1.6 interface policy deny

Syntax

interface policy deny

undo interface policy deny

デフォルト

ユーザは、すべてのインタフェースを操作する権限があります。

View

ユーザロールビュー

定義済みユーザロール

network-admin

説明

interface policy deny コマンドを使用して、インタフェースポリシービューにアクセスします。

undo interface policy deny コマンドを使用して、デフォルトの状態を復元します。

 注意

インタフェースポリシービューにアクセスすると、アクションを許可するインタフェースのリストが設定されていない場合、ユーザはどのインタフェースにもアクションを許可されません。インタフェースリソースに対するユーザの使用権限を制限または区別する必要がある場合は、**permit interface** コマンドを使用して、ユーザが操作できるインタフェースのリストも設定する必要があります。

アクションを許可するインタフェースのリストがインタフェースポリシービューで設定されていない場合、ユーザはすべてのインタフェースをアクションできません。インタフェースの操作とは、インタフェースを作成し、インタフェースの表示、削除、および適用を行うことです。ここで、インタフェースは論理インタフェースに対してのみ作成および削除されます。

ユーザロールのインタフェースポリシーの変更は許可されますが、変更されたポリシーは、ロールを承認されたユーザが再度ログインするまで有効になりません。

例

#ユーザロール role1 で、インタフェースポリシービューに移動し、ロール role1 のユーザがインタフェースを操作できないようにします。

<Sysname> system-view

[Sysname] role name role1

[Sysname-role-role1] interface policy deny

[Sysname-role-role1-ifpolicy] quit

#ユーザロール role1 で、インタフェースポリシービューに入り、ロール role1 のユーザアクションインターフェース GigabitEthernet1/0/1 から GigabitEthernet1/0/4 を許可します。

<Sysname> system-view

[Sysname] role name role1

[Sysname-role-role1] interface policy deny

[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 to gigabitethernet 1/0/4

関連コマンド

- display role
- permit interface
- role

2.1.7 permit interface

Syntax

permit interface *interface-list*

undo permit interface *[interface-list]*

デフォルト

インタフェースインターフェースポリシービューの下にアクションを許可するインタフェースのリストが定義されておらず、ユーザにはどのインタフェースにもアクションを許可する権限がありません。

View

インタフェースポリシービュー

定義済みユーザロール

network-admin

パラメータ

interface interface-list: 10 個までのインタフェース項目をスペースで区切って指定します。各インタフェース項目は、interface-type interface-number 形式でインタフェースを 1 つ指定するか、interface-type interface-number 形式でインタフェースの範囲を指定します。インタフェース範囲を指定する場合、終了インタフェースは次の要件を満たしている必要があります。

- スタートインタフェースと同じタイプであること。
- スタートインタフェースより高いインタフェース番号を持っている。

説明

permit interface コマンドを使用して、ユーザが操作できるインタフェースのリストを設定します。

undo permit interface コマンドは、指定されたインタフェースまたはすべてのインタフェースをユーザが操作できないようにするために使用します。

interface policy deny コマンドを使用してインタフェースポリシービューにアクセスした後、このコマンドを使用して操作を許可するインタフェースのリストを設定する必要があります。

インタフェースの操作とは、インタフェースビューの作成と入力、インタフェースの削除、および適用です。ここで、インタフェースは論理インタフェースに対してのみ作成および削除されます。

このコマンドを複数回実行すると、ユーザが操作できるインタフェースをインタフェースのリストに追加できます。**undo permit interface** コマンド interface-list パラメータを指定しない場合、ユーザはすべてのインタフェースを操作できません。

変更されたインタフェースの資源制御ポリシーは、現在オンラインになっているユーザには適用されず、後でそのロールを使用してデバイスにログインしたユーザには適用されません。

例

#ユーザロール role1 を作成し、ビューに移動します。

<Sysname> system-view

[Sysname] role name role1

#ユーザロールルール 1 を設定して、ユーザがインタフェースビューとインタフェースビューの両方で関連するコマンドを実行できるようにします。

[Sysname-role-role1] rule 1 permit command system-view ;interface *

#ユーザロールルール 2 を設定すると、ユーザは VLAN の作成後に関連するコマンドを実行し、VLAN ビューにアクセスできます。

[Sysname-role-role1] rule 2 permit command system-view ;vlan *

#ユーザロールの設定 role1 は、インタフェースインタフェース GigabitEthernet1/0/1 および GigabitEthernet1/0/3~GigabitEthernet1/0/5 に対してのみ実行できます。

[Sysname-role-role1] interface policy deny

[Sysname-role-role1-ifpolicy] permit interface gigabitethernet 1/0/1 gigabitethernet 1/0/3 to gigabitethernet 1/0/5

ユーザの役割 role1 を持つユーザがデバイスにログインすると、インタフェース GigabitEthernet1/0/1 および GigabitEthernet1/0/3~GigabitEthernet1/0/5 は操作できますが、他のインタフェースは操作できません。

構成結果は次のように検証されます。

- インタフェース GigabitEthernet1/0/1 ビューに入ります。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1]

- インタフェース GigabitEthernet1/0/5 を VLAN 10 に接続します。

<Sysname> system-view

[Sysname] vlan 10

[Sysname-vlan10] port gigabitethernet 1/0/5

- インタフェース GigabitEthernet1/0/2 ビューにアクセスできません。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/2

Permission denied.

関連コマンド

- display role
- interface policy deny
- role

2.1.8 permit vlan

Syntax

permit vlan *vlan-id-list*

undo permit vlan *[vlan-id-list]*

デフォルト

VLAN インタフェースビューでは、操作を許可する VLAN のリストが定義されておらず、ユーザには VLAN を操作する権限がありません。

View

VLAN ポリシービュー

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: ユーザが操作できる VLAN のリスト。vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>で表され、vlan-id は 1~4094 の範囲の値をとり、&<1-10>は前のパラメータを 10 回まで繰り返し入力できることを示します。終端 VLAN 番号は、開始 VLAN 番号より大きい必要があります。

説明

permit vlan コマンドを使用して、ユーザが操作できる VLAN のリストを設定します。

undo permit vlan コマンドは、指定された VLAN またはすべての VLAN に対するユーザアクションを禁止するために使用します。

vlan policy deny コマンドを使用して VLAN ポリシービューにアクセスした後、このコマンドを使用して操作を許可する VLAN のリストを設定して、ユーザが適切な VLAN を操作できるようにする必要があります。

VLAN の操作とは、VLAN を作成して VLAN ビューに移動し、VLAN を削除して適用することです。

このコマンドを複数回実行すると、ユーザが操作できる複数の VLAN を VLAN リストに追加できます。

undo permit vlan コマンド vlan-id-list パラメータを指定しない場合、ユーザはすべての VLAN を操作できません。

変更された VLAN 資源制御ポリシーは、現在オンラインになっているユーザには適用されず、その後そのロールを使用してデバイスにログインしたユーザには適用されません。

デフォルトでは、デバイス上のすべての access ポートは VLAN 1 に属します。**port access vlan** コマンドを使用して access ポートを指定された別の VLAN に結合する場合、このロールには VLAN 1 の操作権限(コマンド permit vlan 1 を使用した設定)も必要です。

例

#ユーザロール role1 を作成し、ビューに移動します。

<Sysname> system-view

[Sysname] role name role1

#ユーザロールルール 1 を設定して、ユーザがインタフェースビューとインタフェースビューの両方で関連するコマンドを実行できるようにします。

[Sysname-role-role1] rule 1 permit command system-view ;interface *

#ユーザロールルール 2 を設定すると、ユーザは VLAN の作成後に関連するコマンドを実行し、VLAN ビューにアクセスできます。

[Sysname-role-role1] rule 2 permit command system-view ;vlan *

#ユーザロールの設定 role1 VLAN 1、VLAN 2、VLAN 4、VLAN 50~VLAN 100 のみを操作できます。

[Sysname-role-role1] vlan policy deny

[Sysname-role-role1-vlanpolicy] permit vlan 1 2 4 50 to 100

ユーザロール role1 を持つユーザがデバイスにログインすると、VLAN 1、VLAN 2、VLAN 4、VLAN 50~VLAN 100 は操作できますが、他の VLAN は操作できません。

構成結果は次のように検証されます。

- VLAN 100 ビューを作成して開きます。

<Sysname> system-view

[Sysname] vlan 100

[Sysname-vlan100]

- Access タイプのポート GigabitEthernet1/0/1 を VLAN 100 に追加します。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] port access vlan 100

- VLAN 101 を作成したり、ビューに移動することはできません。

<Sysname> system-view

[Sysname] vlan 101

Permission denied.

関連コマンド

- display role
- role
- vlan policy deny

2.1.9 role

Syntax

role name *role-name*

undo role name *role-name*

デフォルト

システム定義のユーザロールは、network-admin、network-operator、level-n (n は 0~15 の整数)、security-audit、guest-manager です。

View

System view

定義済みユーザロール

network-admin

パラメータ

name *role-name*:ユーザロール名、role-name は 1~63 文字の文字列で、大文字と小文字が区別されます。

説明

role コマンドを使用して、ユーザロールを作成し、ユーザロールビューに移動します。指定したユーザの役割がすでに存在する場合は、 「ユーザの役割」 ビューに直接移動します。

undo role コマンドは、指定されたユーザロールを削除するために使用します。

システムで事前定義されているデフォルトのユーザロールに加えて、最大 64 個のユーザロールを作成できます。

デフォルトのユーザロールは削除できません。また、network-admin、network-operator、level-15、security-audit、guest-manager の各ユーザロールに定義されているすべての権限は変更できません。ユーザの役割 level-0~level-14 は、カスタムルールと資源制御ポリシーを使用して自身の権限を調整できますが、**display history-command all** コマンドではこの変更は有効になりません。つまり、対応するルールを追加してデフォルトの実行権限を変更することはできません。

非 AAA 認証ユーザにセキュリティログ管理者ロールを付与することはできません。

例

#ユーザロール role1 を作成し、ユーザロールビューに移動します。

<Sysname> system-view

[Sysname] role name role1

[Sysname-role-role1]

関連コマンド

- display role
- interface policy deny
- rule
- vlan policy deny

2.1.10 role default-role enable

Syntax

role default-role enable *[role-name]*

undo role default-role enable

デフォルト

デフォルトのユーザロール機能は無効になっています。ユーザロールをお持ちでない AAA ユーザは、デバイスにログインできません。

View

System view

定義済みユーザロール

network-admin

vsys-admin

パラメータ

role-name:デフォルトのユーザロール名。1~63 文字の文字列で、大文字と小文字が区別されます。システムにすでに存在するユーザロールでもかまいません。

説明

role default-role enable コマンドは、デフォルトのユーザロール認可機能を有効にするために使用します。

undo role default-role enable コマンドを使用して、デフォルトの状態を復元します。

AAA 認証を使用してデバイスにログインしたユーザには、サーバ(リモート認証サーバまたはローカル認証サーバ)が対応するユーザロールを付与します。ユーザにユーザロールが付与されていない場合、デバイスに正常にログインできません。ローカルユーザまたはユーザグループの認証プロパティが **authorization-attribute** コマンドで設定されていない場合は、デフォルトのユーザロール認証機能を有効にする必要があります。この機能を有効にすると、ユーザは、サーバからユーザの役割を委任されることなく、デフォルトのユーザの役割を持つことになります。

ユーザが AAA 認証を受け、特定のユーザロールを付与されている場合、ユーザはデフォルトのユーザロールを持ちません。

role-name パラメータを指定しない場合、デフォルトのユーザロールは network-operator です。

例

#デフォルトのユーザロール承認機能を有効にします。

<Sysname> system-view

[Sysname] role default-role enable

関連コマンド

- role

2.1.11 role feature-group

Syntax

role feature-group name *feature-group-name*

undo role feature-group name *feature-group-name*

デフォルト

L 2 と L 3 という名前の 2 つの機能グループがあります。

View

System view

定義済みユーザロール

network-admin

パラメータ

name *feature-group-name*:プロパティグループ名、feature-group-name は 1~31 文字の文字列で、大文字と小文字が区別されます。

説明

role feature-group コマンドを使用して、プロパティグループを作成し、プロパティグループビューに移動します。指定したプロパティグループがすでに存在する場合は、プロパティグループビューに直接移動します。

undo role feature-group コマンドを使用して、指定した機能グループを削除します。

システム定義の特性グループ L 2 と L 3 に加えて、最大 64 個の特性グループを作成できます。

システム定義の機能グループ L 2 および L 3 は変更および削除できません。L 2 にはすべてのレイヤ 2 プロトコル関連機能のコマンドが含まれ、 L 3 にはすべてのレイヤ 3 プロトコル関連機能のコマンドが含まれる。

例

#プロパティグループ security-features を作成し、プロパティグループビューに移動します。

<Sysname> system-view

[Sysname] role feature-group name security-features

[Sysname-featuregrp-security-features]

関連コマンド

- display role feature
- display role feature-group
- feature

2.1.12 rule

Syntax

rule *number* { **deny** | **permit** } { **command** *command-string* | { **execute** | **read** | **write** } * { **feature** [*feature-name*] | **feature-group** *feature-group-name* | **oid** *oid-string* | **web-menu** [*web-string*] | **xml-element** [*xml-string*] } }

undo rule { *number* | **all** }

デフォルト

新しく作成されたユーザロールには規則が定義されていません。つまり、現在のユーザロールには権限がありません。

View

ユーザロールビュー

定義済みユーザロール

network-admin

パラメータ

number:権限ルール番号。範囲は 1~256 です。

deny:指定したコマンド、Web メニュー、XML 要素、または MIB ノード OID の実行を禁止します。

permit:指定したコマンド、Web メニュー、XML 要素、または MIB ノード OID を実行できます。

command *command-string*:コマンドベースのルールを設定します。command-string は、コマンドの特性を示す 1~128 文字の文字列です。大文字と小文字が区別され、特定のコマンドラインまたはアスタリスク (*) のワイルドカードを使用して、スペース、タブ(キーワード、パラメータ、および入力した文字を区切るために使用されます。)、印刷可能なすべての文字を含む一連のコマンドを表すことができます。コマンドフィーチャー文字列に[」 または 「」]文字が含まれている場合は、エスケープ文字 「¥」 を付加する必要があります。たとえば、コマンドフィーチャー文字列が statistics [ifindex="*"]の場合、statistics¥[ifindex="*"¥]と入力します。

execute:実行タイプを表すコマンド、Web メニュー、XML 要素、または MIB ノード OID。特定のプログラムや機能を実行したり、ping コマンドなどのコマンドを実行したりできます。

read:読み込みタイプを表すコマンド、Web メニュー、XML 要素、または MIB ノード OID。システム構成とメンテナンス情報を表示します。読み取りタイプには、display、dir、more、pwd コマンドなどのコマンドがあります。

write:書き込みタイプを表すコマンド、Web メニュー、XML 要素、または MIB ノード OID。システムの構成に使用されます。書き込みタイプのコマンドは ssh server enable のようになります。

feature *[feature-name]*:属性ベースのルールを設定します。feature-name は、システム定義プロパティ名で、大文字と小文字が区別されます。プロパティ名を指定しない場合は、すべてのプロパティが表示されます。

feature-group *feature-group-name*:プロパティグループに基づくルールを設定します。feature-group-name は、プロパティグループ名を示す 1~31 文字の文字列で、大文字と小文字が区別されます。プロパティグループに基づく規則は、プロパティグループが作成されるまで有効になりません。作成したプロパティグループ情報を表示するには、display role feature-group コマンドを使用します。

oid *oid-string*:MIB ノードの OID (Object Identifier、オブジェクト識別子)に基づいてルールを構成します。oid-string は、操作を許可する OID を表し、大文字と小文字を区別しない 1~255 文字の文字列です。OID は、MIB ツリー内のノードの位置を示す一連の整数で構成され、MIB ライブラリ内のオブジェクトを一意に識別します。例:1.3.6.1.4.1.25506.8.35.14.19.1.1。

web-menu *[web-string]*:Web メニューベースのルールを設定します。web-string は、操作が許可されている Web メニューオプションの ID パスを表します。1~255 文字の文字列で、大文字と小文字は区別されません。メニューのレベルは 「/」 で区切ります。正当な web-string は display web menu コマンドによって表示される ID パスです例:M_DEVICE/I_BASIC_INFO/I_reboot;web-string パラメータを指定しない場合は、すべてのメニューオプションが有効になります。

xml-element *[xml-string]*:XML 要素に基づく規則を設定します。xml-string は、操作を許可する XML 要素を表す XPath で、大文字と小文字を区別しない 1~255 文字の文字列です。 「/」 は、メニューのレベルを区切るための区切り文字です。例:Interfaces/Index/Name;xml-string パラメータを指定しない場合は、すべての XML 要素に対して有効です。

all:すべての権限規則を指定します。

説明

rule コマンドを使用して、ユーザロールの規則を作成します。

undo rule コマンドは、ユーザロールのルールを削除するために使用します。

アクセスコントロールの粒度ごとに、次のタイプのルールを定義できます。

- コマンド規則:正規表現に一致するコマンドまたはコマンドセットへのアクセスを制御します。
- 機能規則:機能のコマンドへのアクセスをコマンドタイプ別に制御します。
- 機能グループ規則:機能グループのコマンドへのアクセスをコマンドタイプ別に制御します。

- Web メニュー規則:メニュータイプ別に Web メニューへのアクセスを制御します。
- XML 要素規則:要素タイプ別に XML 要素へのアクセスを制御します。
- OID 規則:指定した MIB ノードとその子ノードへのアクセスをノードタイプ別に制御します。

ユーザロールは、ユーザロールルールで指定された許可されたリソースのセットにアクセスできます。ユーザロール規則には、定義済み (sys-n で識別される) およびユーザ定義のユーザロール規則があります。

ユーザロールには最大 256 のユーザ定義ルールを設定できます。ユーザ定義のユーザロールルールの合計数は 1024 を超えることはできません。

ユーザロールに対するルールの変更、追加、または削除は、変更後にユーザロールでログインするユーザに対してのみ有効になります。

ファイルシステムコマンドへのアクセスは、ファイルシステムコマンド規則とファイルシステム機能規則の両方によって制御されます。

ファイルシステムへの出力リダイレクトを持つコマンドは、コマンドタイプ write がファイルシステム機能に割り当てられている場合にのみ許可されます。

次のガイドラインが非 OID ルールに適用されます。

- 同じタイプの 2 つのユーザ定義ルールが競合する場合は、ID が大きい方のルールが有効になります。たとえば、ユーザロールに次のコマンドを使用して設定されたルールが含まれている場合、ユーザロールは tracert コマンドを使用できますが、ping コマンドは使用できません。
  - **rule** *1* **permit command** *ping*
  - **rule** *2* **permit command** *tracert*
  - **rule** *3* **deny command** *ping*
- 事前定義されたユーザロールルールとユーザ定義のユーザロールルールが競合する場合は、ユーザ定義のユーザロールルールが有効になります。

次のガイドラインが OID 規則に適用されます。

- システムは、ルールで指定された OID と OID を比較し、最長一致原則を使用して OID のルールを選択します。たとえば、次のコマンドを使用して設定されたルールがユーザロールに含まれている場合、ユーザロールは OID 1.3.6.1.4.1.25506.141.3.0.1 の MIB ノードにアクセスできません。
  - **rule** *1* **permit read write oid** *1.3.6*
  - **rule** *2* **deny read write oid** *1.3.6.1.4.1*
  - **rule** *3* **permit read write oid** *1.3.6.1.4*
- 複数のルールで同じ OID を指定した場合は、ID が大きい方のルールが有効になります。たとえば、次のコマンドを使用して設定されたルールがユーザロールに含まれている場合、ユーザロールは OID 1.3.6.1.4.1.25506.141.3.0.1 を持つ MIB ノードにアクセスできます。
  - **rule** *1* **permit read write oid** *1.3.6*
  - **rule** *2* **deny read write oid** *1.3.6.1.4.1*

- **rule** *3* **permit read write oid** *1.3.6.1.4.1*

- コマンド文字列を指定する場合は、表 2-4 のガイドラインに従ってください。

表 2-4 コマンド文字列設定規則

ルール	ガイドライン
セミコロン (;) はデリミタである。	コマンドまたは一連のコマンドにアクセスする前に入力する必要がある各ビューのコマンドは、セミコロンで区切ります。ただし、user viewやその他のビューで使用できるコマンド (displayやdirなど) を区切るためにセミコロンを使用しないでください。 セミコロンで区切られた各セグメントには、少なくとも1つの印刷可能な文字が必要です。 ビュー内のコマンドを指定し、ビューのサブビュー内のコマンドを指定しない場合は、最後のセグメントの最後の印刷可能文字としてセミコロンを使用します。ビュー内のコマンドとビューのサブビューを指定するには、最後のセグメントの最後の印刷可能文字をセミコロンにすることはできません。 たとえば、interface viewを入力する前にsystem viewを入力する必要があります。任意のinterface viewでipキーワードで始まるすべてのコマンドを指定するには、「system ; interface * ; ip * ;」コマンド文字列を使用する必要があります。 別の例として、「system ; radius scheme 」コマンド文字列は、system viewでradius schemeキーワードで始まるすべてのコマンドを表します。 「system ; radius scheme 」コマンド文字列は、system viewではradius schemeキーワードで始まるすべてのコマンドを、RADIUSスキームビューではすべてのコマンドを表します。
アスタリスク (*) はワイルドカードです。	アスタリスクは0または複数の文字を表します。 最後以外のセグメントでは、セグメントの最後にのみアスタリスクを使用できます。 最後のセグメントでは、セグメントの任意の位置にアスタリスクを使用できます。先頭に 「*」 がある場合は、その後ろに印字可能文字を指定できません。 たとえば、「system ; *」コマンド文字列は、system viewで使用可能なすべてのコマンドと、system viewのすべてのサブビューを表します。 "debugging*event"コマンド文字列は、user viewで使用可能なすべてのイベントデバッグコマンドを表します。
キーワードの省略は可能です。	キーワードを指定するには、キーワードの最初の数文字を入力します。この文字列で始まるコマンドはすべてルールに一致します。 たとえば、"rule 1 deny command dis arp source*"はコマンドdisplay arp source-mac インタフェースおよびdisplay arp source-suppressionへのアクセスを拒否します。

ルール	ガイドライン
コマンドへのアクセスを制御するには、コマンドを含むビューの直後にコマンドを指定する必要があります。	コマンドへのアクセスを制御するには、コマンドが割り当てられているビューのすぐ後ろにコマンドを指定する必要があります。サブビューのコマンドアクセスを制御する規則は、コマンドには適用されません。 たとえば、「rule 1 deny command system ; interface * ; *」コマンド文字列は、interface viewに割り当てられているすべてのコマンドへのアクセスを無効にします。ただし、このコマンドはinterface viewではなくsystem viewに割り当てられているため、interface viewでacl advancedコマンドを実行することはできます。このコマンドへのアクセスを無効にするには、"rule 1 deny command system;acl*;"。
ユーザロールコマンドルールで表示コマンドを指定する場合は、縦棒 (|) 、大なり記号 (>) 、二重大なり記号 (>>) を含めないでください。	システムは、リダイレクト記号と、記号に続くパラメータをコマンドラインの一部として扱いません。ただし、ユーザロールコマンドルールでは、これらのリダイレクト記号とパラメータはコマンドラインの一部として扱われます。その結果、これらの符号のいずれかを含むルールは一致を見つけることができません。 たとえば、"rule 1 permit command display debugging>log"は一致を見つけることができません。これは、システムにはdisplay debuggingコマンドはあるが、display debugging>logコマンドがないためです。

例

#ユーザロール role1 に対して、ユーザがコマンド display acl を実行できるようにする規則を作成します。

<Sysname> system-view

[Sysname] role name role1

[Sysname-role-role1] rule 1 permit command display acl

#ユーザロール role1 にアクセス許可規則を追加し、ユーザが display で始まるすべてのコマンドを実行できるようにします。

[Sysname-role-role1] rule 2 permit command display *

#ユーザロール role1 にアクセス許可規則を追加して、ユーザがシステムビューで radius scheme aaa コマンドを実行できるようにし、そのコマンドを使用してサブビューに移動するすべてのコマンドを実行できるようにします。

[Sysname-role-role1] rule 3 permit command system ;radius scheme aaa

#すべてのプロパティの読み取りタイプと書き込みタイプのコマンドを実行できないようにするために、ユーザロール role1 にアクセス許可規則を追加します。

[Sysname-role-role1] rule 4 deny read write feature

#プロパティ aaa のすべての読み取りタイプのコマンドを実行できないようにするユーザロール role1 のアクセス許可規則を追加します。

[Sysname-role-role1] rule 5 deny read feature aaa

#プロパティグループ security-features のすべてのプロパティの読み取り、書き込み、および実行タイプのコマンドの実行を許可するユーザロール role1 のアクセス許可規則を追加します。

[Sysname-role-role1] rule 6 permit read write execute feature-group security-features

#ユーザロール role1 に OID ベースのルールを追加し、OID が 1.1.2 の MIB ノードに対する読み取りと書き込みを許可します。

[Sysname-role-role1] rule 7 permit read write oid 1.1.2

関連コマンド

- display role
- display role feature
- display role feature-group
- display web menu (基本設定コマンドリファレンス/ログインデバイス)
- role

2.1.13 super

Syntax

super *[role-name]*

View

ユーザビュー

定義済みユーザロール

network-admin

パラメータ

role-name:切り替えられるユーザの役割の名前。1~63 文字の文字列で、大文字と小文字が区別されます。security-audit、guest-manager 以外のシステムにすでに存在するユーザの役割を指定できます。このパラメータを指定しない場合は、現在のデフォルトのダイナミックユーザロールに切り替えます。デフォルトのダイナミックユーザロールは、**super default role** コマンドで指定されます。

説明

super コマンドは、ユーザを現在のロールから指定されたユーザロールに切り替えるために使用します。

切り替え後のユーザの役割は現在のログインに対してのみ有効になり、ユーザが再度ログインすると元の役割に戻ります。

操作の安全性を確保するため、通常、ユーザがユーザロールの切替えを行う際には、ユーザロール切替えパスワードの入力が必要となる。別のユーザの役割に切り替えるには、

適切な切り替えパスワードを入力する必要があります。サーバが応答しないか、ユーザの役割のスイッチオーバーパスワードが設定されていない場合、スイッチオーバー操作は失敗し、バックアップ認証スキームがある場合は、バックアップ認証に移行します。したがって、スイッチオーバー操作を実行する前に、正しいユーザロールスイッチオーバーパスワードが設定されていることを確認してください。

ユーザの役割を切り替えるときは、次の点に注意してください。

- レベル切換認証方式が local であり、機器に切換パスワードが設定されていない場合、AUX ユーザに対して、機器は、ユーザが切換パスワードを入力したか否か及び入力した切換パスワードの内容に関わらず、ユーザがユーザの役割を正常に切換できるようにすることができる。
- レベル切替認証方式が local scheme であり、機器に切替パスワードが設定されていない場合、VTY ユーザに対しては、リモート AAA 認証に移行する;AUX ユーザの場合、デバイスは、ユーザがスイッチオーバーパスワードを入力したかどうか、および入力されたスイッチオーバーパスワードの内容には関係なく、ユーザがユーザの役割を正常にスイッチオーバーできるようにします。

例

#ユーザの役割を network-operator に切り替えます。(ユーザの現在の役割が network-admin、切り替え認証方式が local で、切り替えパスワードが設定されているとします。)

<Sysname> super network-operator

```
Password:
User privilege role is network-operator、and only those commands that authorized to the role can be used.
```

関連コマンド

- authentication super (ユーザアクセスおよび認証コマンドリファレンス/AAA)
- super authentication-mode
- super password

2.1.14 super authentication-mode

Syntax

super authentication-mode { **local** | **scheme** } *

undo super authentication-mode

デフォルト

local 認証方式を採用している。

View

System view

定義済みユーザロール

network-admin

パラメータ

local:ローカルに設定されたユーザロールスイッチパスワードを使用して認証します。

scheme 認証に AAA 設定を使用します。

説明

super authentication-mode コマンドは、ユーザの役割を切り替えるときに使用する認証方式を設定します。

undo super authentication-mode コマンドを使用して、デフォルトの状態を復元します。

ローカルパスワード認証を使用する場合は、**super password** コマンドを使用して、ユーザの役割を切り替えるためのパスワードをデバイスに設定する必要があります。

リモート AAA 認証を使用する場合は、RADIUS または HWTACACS サーバでユーザ名とユーザロールスイッチパスワードを設定する必要があります。

ユーザは local または scheme 方式で認証するか、 local と scheme 方式を同時に選択するかを選択でき、複数選択した場合は配置順に順次認証する。

- local scheme 方式:先にローカルパスワード認証を行い、もし設備にローカルユーザ役割切り替えパスワードを設置しなければ、AUX 或は VTY ユーザ線でログインするユーザはリモート AAA 認証に転換する。
- scheme local 方式:先にリモート AAA 認証を行うが、リモート HWTACACS/RADIUS サーバが応答しない場合やデバイス上の AAA リモート認証設定が無効な場合は、ローカルパスワード認証に切り替える。

scheme 認証方式は AAA の認証スキームと組み合わせる必要があり、詳しくは QX-W2300 AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

例

#スイッチユーザの役割を設定する場合は、local 認証を使用します。

<Sysname> system-view

[Sysname] super authentication-mode local

#スイッチユーザの役割を設定するときは、scheme の後に local を指定します。

<Sysname> system-view

[Sysname] super authentication-mode scheme local

関連コマンド

- authentication super (ユーザアクセスと認証-AAA)
- super password

2.1.15 super default role

Syntax

super default role *role-name*

undo super default role

デフォルト

ユーザロールスイッチのデフォルトのダイナミックロールは network-admin です。

View

System view

定義済みユーザロール

network-admin

パラメータ

role-name:切り替えられるユーザの役割の名前。1~63 文字の文字列で、大文字と小文字が区別されます。security-audit、guest-manager 以外のシステムにすでに存在するユーザの役割を指定できます。

説明

super default role コマンドを使用して、ユーザロールの切り替えを構成するデフォルトのダイナミックロール。

undo super default role コマンドを使用して、デフォルトの状態を復元します。

ユーザの役割を切り替えるために **super** コマンドを実行する場合、またはユーザの役割を切り替えるためのパスワードを構成する場合、目的のスイッチの役割名を指定しないと、**super default role** コマンドを使用して構成されたデフォルトのユーザの役割が表示されます。

例

#ユーザスイッチロールを構成するデフォルトのダイナミックロールは network-operator です。

<Sysname> system-view

[Sysname] super default role network-operator

関連コマンド

- super
- super password

2.1.16 super password

Syntax

super password [role *role-name* **] [{hash |simple }** *string* **]**

undo super password [role *role-name* **]**

デフォルト

ユーザロール切り替えパスワードが設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

role *role-name*:切り替えるユーザロールの名前。1~63 文字の文字列で、大文字と小文字が区別されます。security-audit、guest-manager 以外のシステムにすでに存在する任意のユーザロールを指定できます。ロール名を指定しない場合は、現在のデフォルトのダイナミックユーザロールに切り替えるためのパスワードが設定されます。デフォルトのダイナミックユーザロールは、**super default role** コマンドで指定されます。

hash:パスワードをハッシュで設定します。

simple:ハッシュ化された暗号化テキストとして保存されるパスワードをクリアテキストで設定します。

string:大文字と小文字を区別するパスワード文字列。平文パスワードが 1~63 文字の文字列;ハッシュパスワード 1~110 文字の文字列。

説明

super password コマンドは、ユーザロールの切り替えに使用するパスワードを設定します。

undo super password コマンドは、ユーザロール切り替えパスワードを削除するために使用します。hash 引数または simple 引数を指定しない場合、**super password [role role-name]**コマンドは、simple キーワードを指定した場合と同じ意味で、ローカルユーザのパスワードを対話形式で設定します。

このコマンドで指定したユーザロール切り替えパスワードは、ユーザ切り替え認証方式が local の場合、または local (local scheme、scheme local)を含む場合にのみ必要です。

権限制御をより安全にするために、異なるスイッチオーバーパスワードを異なるユーザロールに割り当てることを推奨します。

履歴パスワードは、グローバル Password Control 機能がオンの状態で継続的に記録されます。新しいユーザロールをクリアテキストで設定するパスワードを切り替える場合、新しいパスワードがすべての履歴パスワードおよび現在のパスワードと異なることを確

認する必要があります。新しいユーザロールをハッシュ化してパスワードを切り替えると、新しいパスワードは履歴パスワードと現在のパスワードと比較されず、同じパスワードでも異なるパスワードでもかまいません。

例

#設定ユーザロールを network-operator に切り替えるときに使用するパスワードは、クリアテキストのパスワード 123456 TESTplat&!です。

<Sysname> system-view

[Sysname] super password role network-operator simple 123456TESTplat&!

#ユーザロールを network-operator に切り替えるときに使用するパスワードを、クリアテキストのパスワード 123456 TESTplat&!に対話形式で設定します。

<Sysname> system-view

[Sysname] super password role network-operator

```
Password:
Confirm :
Updating user information.Please wait ......
```

関連コマンド

- super authentication-mode
- super default role

2.1.17 vlan policy deny

Syntax

vlan policy deny

undo vlan policy deny

デフォルト

ユーザには、任意の VLAN を操作する権限があります。

View

ユーザロールビュー

定義済みユーザロール

network-admin

説明

vlan policy deny コマンドを使用して、VLAN policy view にアクセスします。

undo vlan policy deny コマンドを使用して、デフォルトの状態を復元します。

注意

permit vlan コマンドが設定されていない場合、**vlan policy deny** コマンドは、すべての VLAN へのユーザロールのアクセスを拒否します。

ユーザロールの VLAN アクセスを一連の VLAN に制限するには、次のタスクを実行します。

1. **vlan policy deny** コマンドでユーザロールの VLAN policy ビューへ移行します。
2. **permit vlan** コマンドでアクセス可能な VLAN を指定します。

VLAN を設定するため、ユーザロールの VLAN ポリシーで許可されている VLAN が使用されていることを確認してください。アクセス可能な VLAN で以下の操作を実行することができます。

- VLAN の作成、削除、設定を行います。
- VLAN ビューへ移行します。
- feature コマンドで VLAN を指定します。

ユーザロールの VLAN ポリシーの変更は、変更後にユーザロールにログインしたユーザのみ適用されます。

例

#ユーザロール role1 で、VLAN policy ビューに入り、ロール role1 のユーザが任意の VLAN を操作できないようにします。

<Sysname> system-view

[Sysname] role name role1

[Sysname-role-role1] vlan policy deny

[Sysname-role-role1-vlanpolicy] quit

#ユーザロール role1 で、VLAN policy ビューに入り、ロール role1 のユーザが VLAN 50~VLAN 100 を操作できるようにします。

<Sysname> system-view

[Sysname] role name role1

[Sysname-role-role1] vlan policy deny

[Sysname-role-role1-vlanpolicy] permit vlan 50 to 100

関連コマンド

- display role
- permit vlan
- role

目次

このセクションのページは **2-x-x** です。

3 章 ログイン管理 3-1
3.1 ログイン管理コマンド 3-1
3.1.1 authentication-mode 3-1
3.1.2 auto-execute command 3-3
3.1.3 databits 3-5
3.1.4 display line 3-6
3.1.5 display telnet client 3-8
3.1.6 display user-interface 3-9
3.1.7 display users 3-11
3.1.8 display web menu 3-12
3.1.9 display web users 3-13
3.1.10 escape-key 3-14
3.1.11 free line 3-17
3.1.12 free user-interface 3-18
3.1.13 free web users 3-19
3.1.14 history-command max-size 3-19
3.1.15 http url allowlist 3-21
3.1.16 http acl 3-22
3.1.17 https acl 3-23
3.1.18 idle-timeout 3-25
3.1.19 line 3-26
3.1.20 line class 3-27
3.1.21 lock 3-28
3.1.22 parity 3-29
3.1.23 protocol inbound 3-30
3.1.24 screen-length 3-32
3.1.25 send 3-33
3.1.26 set authentication password 3-34
3.1.27 shell 3-36
3.1.28 speed 3-37
3.1.29 stopbits 3-37
3.1.30 telnet 3-38
3.1.31 telnet client source 3-39
3.1.32 telnet server acl 3-40
3.1.33 telnet server dscp 3-42
3.1.34 telnet server enable 3-42

3.1.35 telnet server port 3-43
3.1.36 terminal type 3-44
3.1.37 user-interface 3-45
3.1.38 user-interface class 3-46
3.1.39 user-role 3-48
3.1.40 web idle-timeout 3-49

3章 ログイン管理

3.1 ログイン管理コマンド

User line view と User line class view の両方をサポートするコマンドの場合、このドキュメントのコマンド説明では、User line view でのコマンドの動作についてのみ説明します。User line class view でのコマンドの動作については、次の規則に従ってください。

- User line view の設定はその User line にのみ有効で、User line class view の設定はその User line に有効です。
- デフォルト以外の構成がデフォルト構成より優先されます。User line view と User line class view の両方でデフォルト以外の設定が使用されている場合、User line view の設定が User line class view の設定より優先されます。
- User line class view での設定の変更は、ユーザが次回ログインしたときに変更された設定値にすぐには反映されません。

3.1.1 authentication-mode

Syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

デフォルト

Console からログインする場合の認証方式は none で、ユーザは直接ログインできます。

VTY 加入者線経由で機器にログインする認証方式は password。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

none:認証は行われません。

password:パスワード認証を行う方式。

scheme:AAA 認証方式を行う。AAA については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

説明

authentication-mode コマンドは、ユーザがデバイスにログインするときの認証方法を設定します。

undo authentication-mode コマンドを使用して、デフォルトの状態を復元します。

 注意

- 認証を無効にすると、ユーザは認証なしでログインできます。セキュリティ上の理由から、認証は慎重に無効にしてください。
- パスワード認証を有効にする場合は、line または line class の認証パスワードも設定する必要があります。認証パスワードが設定されていない場合、次回に line または line class を使用してデバイスにログインすることはできません。
- スキーム認証を有効にする場合は、認証ユーザアカウントが使用可能であることを確認します。使用可能な認証ユーザアカウントがない場合、次回に line または line class を使用してデバイスにログインすることはできません。

このコマンドを実行できるのは、network-admin またはレベル 15 のユーザロールを割り当てられたユーザだけです。このコマンドを実行する権限が付与されていても、他のユーザはこのコマンドを実行できません。

VTY line view では、このコマンドは protocol inbound コマンドに関連付けられています。

- VTY line view の 2 つのコマンドの設定が両方ともデフォルト設定の場合、VTY line class view のコマンドの設定が有効になります。
- VTY line view の 2 つのコマンドの設定が両方ともデフォルト以外の設定の場合、VTY line view のデフォルト以外の設定が有効になります。
- VTY line view のデフォルト以外の設定を持つコマンドが 1 つだけの場合、もう 1 つのコマンドは VTY line class view の設定に関係なく、デフォルト設定を使用します。

認証モードの変更は、現在のセッションでは有効になりません。後続のログインセッションで有効になります。

例

#VTY 0 の加入者線を使用してデバイスにログインするようにユーザを設定する場合、認証は必要ありません。

```
<AC> system-view
[AC] line vty 0
[AC-line-vty0] authentication-mode none
```

#ユーザが VTY 0 の加入者線を使用してデバイスにログインするように設定するには、パスワード認証が必要で、認証パスワードは hello12345 です。

```
<AC> system-view
```

[AC] line vty 0
[AC-line-vty0] authentication-mode password
[AC-line-vty0] set authentication password simple hello12345

#ユーザのセットアップ VTY 0 user line を使用して、ローカル AAA 認証を使用してデバイスに Telnet でログインします。ユーザ名は test、認証パスワードは hello12345、サービスタイプは Telnet、ユーザロールは network-admin です。

<AC> system-view
[AC] line vty 0
[AC-line-vty0] authentication-mode scheme
[AC-line-vty0] quit
[AC] local-user test
[AC-luser-manage-test] password simple hello12345
[AC-luser-manage-test] service-type telnet
[AC-luser-manage-test] authorization-attribute user-role network-admin

関連コマンド

- set authentication password

3.1.2 auto-execute command

Syntax

auto-execute command *command*

undo auto-execute command

デフォルト

自動実行コマンドが設定されていません。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

command:自動的に実行する必要があるコマンド。

説明

auto-execute command コマンドは、自動実行コマンドを設定します。

undo auto-execute command コマンドを使用して、デフォルトの状態を復元します。

注意

user line にこのコマンドを実行すると、user line による CLI アクセスができなくなる可能性があります。このコマンドを設定する前に、異なる user line によって CLI にアクセスできることを確認してください。

ユーザが User line を介してログインすると、デバイスは指定されたコマンドを自動的に実行し、コマンドの実行後にユーザ接続を閉じます。

このコマンドは、AUX line view または AUX line class view で使用できます。

このコマンドは、User line view と User line class view の両方で使用できます。どちらかの view のデフォルト以外の設定は、もう一方の view のデフォルト設定よりも優先されます。User line view のデフォルト以外の設定は、User line class view のデフォルト以外の設定よりも優先されます。

このコマンドによって行われた設定変更は、現在のセッションでは有効になりません。以降のログインセッションで有効になります。

例

#VTY 0 からデバイスにログインするようにユーザを設定すると(IP アドレス 192.168.1.40)、IP アドレスが 192.168.1.41 のデバイスに Telnet が自動的に割り当てられます。

<AC> system-view
[AC] line vty 0
[AC-line-vty0] auto-execute command telnet 192.168.1.41
This action will lead to configuration failure through line-vty0.Are you sure? [Y/N]:y
[AC-line-vty0]

結果の検証:

再度 Telnet にログインすると、自動的に telnet 192.168.1.41 コマンドを実行し、Telnet クライアントに次のメッセージが表示されます。

C:¥>telnet 192.168.1.40

<AC>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...

<AC>

これは、ユーザが 192.168.1.41 デバイスに直接ログインしたことに相当します。ユーザが 192.168.1.41 への Telnet 接続を切断すると、192.168.1.40 デバイスへの Telnet 接続も自動的に切断されます。

3.1.3 databits

Syntax

databits { **7** | **8** }

undo databits

デフォルト

加入者線のデータビットは 8 ビットである。

View

User line view

定義済みユーザロール

network-admin

パラメータ

7:データビットは 7 ビットで、7 ビットを使用して文字を表します。

8:データビットは 8 ビットで、8 ビットを使用して文字を表します。

説明

databits コマンドは、データビットの数を設定します。

undo databits コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、VTYUser line class view ではサポートされていません。

アクセス端末と設備の相応する user line の下のデータビットの設定は双方が正常に通信するために一致しなければならない。

例

#データビットを 7 ビットに設定します。

<AC> system-view
[AC] line aux 0
[AC-line-aux0] databits 7

3.1.4 display line

Syntax

display line [*number1* | { **aux** | **vty** } *number2*] [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

number1: user line の番号(絶対番号付け)。範囲は 0~64 です。

aux:AUX user line。

vty:VTY user line。

number2: user line の番号(相対番号付け)。AUX user line の場合は 0、VTY user line の場合は 0~63 の範囲。

summary: user line の概要情報を表示します。このパラメータを使用しない場合は、加入者線タイプ、絶対/相対番号、伝送速度、認証方式、およびアクセスインタフェースが表示されます。このパラメータを使用すると、使用中および未使用の user line の数とタイプが表示されます。

例

display line コマンドは、 user line に関する情報を表示します。

user line0 に関する情報を表示します。

<AC> display line 0

```
IdxTypeTx/RxModem AuthIntLocation
F 0AUX 09600-N-1/0

+:Line is active.
F:Line is active and in async mode.
Idx:Absolute index of line.
Type :Type and relative index of line.
Auth :Login authentication mode.
Int:Physical port of the line.
A:Authentication use AAA.
N:No authentication is required.
P:Password authentication.
```

表 3-1 display line コマンドの表示情報の説明

フィールド	説明
+	現在使用中の user lineを表します
F	現在使用されており、非同期で動作している加入者線を示します。
Idx	user lineの絶対番号
Type	user lineのタイプと相対番号
Tx/Rx	加入者線の速度
Modem	(未サポート) Modemの着信/発信スイッチ。値はin (着信許可)、out (呼び出しを許可)、inout (着信コールの許可)で、デフォルトは 「-」 (設定されていないことを示します)です。
Auth	この加入者線を利用してログインしたユーザの認証方式は、 A, L, N, Pの4通りの値をとる.
Int	加入者線に対応する物理インタフェースの略称表示(Consoleポートと、対応するインタフェースがない加入者線には 「-」 が表示されます。)
Location	加入者線の物理的位置
A	AAA認証方式を用いていることを示し、対応するauthentication-modeはschemeである.
N	認証不要であることを示し､対応するauthentication-modeはnoneである.
P	現在の加入者線のパスワードを使用して認証することを示します。対応するauthentication-modeはpasswordです。

#すべての加入者線の概要情報を表示します。

<AC> display line summary

```
Line type :[AUX]
0:X
Line type :[VTY]
1:UUUU UUXX XXXX XXXX
17:XXXX XXXX XXXX XXXX
33:XXXX XXXX XXXX XXXX
49:XXXX XXXX XXXX XXXX

6 lines used.(U)
59 lines not used.(X)
```

表 3-2 display line summary コマンドの表示情報の説明

フィールド	説明
Line type	user lineのタイプ: • AUX:AUX user line • VTYはVTYの加入者線

フィールド	説明
0:UXXX XXXX XX	0は user lineの絶対番号です。 Xは、現在ユーザがこの user lineを使用していないことを示します。 Uは、現在ユーザがこの user lineを使用していることを示します。
lines used.(U)	現在使用中の user lineの数(つまり、Uの文字数)
lines not used.(X)	現在使用されていない user lineの数(Xの文字数)

3.1.5 display telnet client

Syntax

display telnet client

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display telnet client コマンドは、Telnet クライアントとしてデバイスの設定情報を表示するために使用されます。

現在、このコマンドは、Telnet クライアントの送信元 IPv 4 アドレスまたは送信元インタフェースの構成情報を表示します。**telnet client source** コマンドを使用して、Telnet クライアントの送信元 IPv 4 アドレスまたは送信元インタフェースを指定できます。

例

#Telnet クライアントとしてデバイスに関連する設定情報を表示します。

<AC> display telnet client

```
The source IP address is 1.1.1.1.
```

上記の表示メッセージは、デバイスが Telnet クライアントである場合、Telnet メッセージを送信する送信元 IPv 4 アドレスが 1.1.1.1 であることを示しています。

関連コマンド

- telnet client source

3.1.6　display user-interface

Syntax

display user-interface [*number1* | { **aux** | **vty** } *number2*] [**summary**]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

number1:User line の番号(絶対番号付け)。範囲は 0~64 です。

aux:AUX user line

vty:VTY user line

number2:User line の番号(相対番号付け)。AUXUser line の場合は 0、VTYUser line の場合は 0~63 の範囲。

summary:User line の概要情報を表示します。このパラメータを使用しない場合は、加入者線タイプ、絶対/相対番号、伝送速度、認証方式、およびアクセスインタフェースが表示されます。このパラメータを使用すると、使用中および未使用の User line の数とタイプが表示されます。

説明

display user-interface コマンドは、User line に関する情報を表示します。

このコマンドの実装は display line に準拠しており、旧バージョンとの互換性のためにのみ予約されています。display line を使用してください。

例

user line0 に関する情報を表示します。

<AC> display user-interface 0

```
IdxTypeTx/RxModem AuthIntLocation
F 0AUX 09600-N-1/0

+:Line is active.
F:Line is active and in async mode.
Idx:Absolute index of line.
Type :Type and relative index of line.
Auth :Login authentication mode.
Int:Physical port of the line.
A:Authentication use AAA.
```

```
N:No authentication is required.
P:Password authentication.
```

表 3-3 display user-interface コマンドの表示情報の説明

フィールド	説明
+	現在使用中の user lineを表します
F	現在使用されており、非同期で動作している加入者線を示します。
Idx	user lineの絶対番号
Type	user lineのタイプと相対番号
Tx/Rx	加入者線の速度
Modem	(未サポート) Modemの着信/発信スイッチ。値はin (着信許可)、out (呼び出しを許可)、inout (着信コールの許可)で、デフォルトは 「-」 (設定されていないことを示します)です。
Auth	この加入者線を利用してログインしたユーザの認証方式は、 A, L, N, Pの4通りの値をとる.
Int	加入者線に対応する物理インタフェースの略称表示(Consoleポートと、対応するインタフェースがない加入者線には 「-」 が表示されます。)
Location	加入者線の物理的位置
A	AAA認証方式を用いていることを示し、対応するauthentication-modeはschemeである.
N	認証不要であることを示し､対応するauthentication-modeはnoneである.
P	現在の加入者線のパスワードを使用して認証することを示します。対応するauthentication-modeはpasswordです。

#すべての加入者線の概要情報を表示します。

<AC> display user-interface summary

```
Line type :[AUX]
0:X
Line type :[VTY]
1:UUUU UUUU UXXX XXXX
17:XXXX XXXX XXXX XXXX
33:XXXX XXXX XXXX XXXX
49:XXXX XXXX XXXX XXXX
9 lines used.(U)
56 lines not used.(X)
```

表 3-4 display user-interface summary コマンドの表示情報の説明

フィールド	説明
Line type	user lineのタイプ: ● AUX:AUX user line ● VTYはVTYの加入者線
0:UXXX XXXX XX	0はUser line の絶対番号です。 Xは、現在ユーザがこの user lineを使用していないことを示します。 Uは、現在ユーザがこの user lineを使用していることを示します。
lines used.(U)	現在使用中の user lineの数(つまり、Uの文字数)
lines not used.(X)	現在使用されていない user lineの数(Xの文字数)

3.1.7 display users

Syntax

display users [**all**]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

all:デバイスがサポートしているすべての加入者線とユーザに関する情報を表示します。

説明

display users コマンドを使用して、使用中の user line とユーザに関する情報を表示します。

例

#使用中の User line とユーザに関する情報を表示します。

<AC> display users

```
  Idx  Line     Idle      Time            Pid     Type
+ 10   VTY 0    00:00:00   Jan 01 00:33:10   484     TEL
  12   VTY 2    00:06:22   Jan 01 00:33:22   495     TEL

Following are more details.
```

```
VTY 0   :
       Location: 192.168.1.107
VTY 2   :
       Location: 192.168.1.134
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

表 3-5 display users コマンドの表示情報の説明

フィールド	説明
Idx	user lineの絶対番号
Line	加入者線の相対番号。最初の列(例:VTY)は加入者線のタイプを表し、2番目の列(例0)は加入者線の相対番号を表します。
Idle	アイドル時間。ユーザとデバイスがメッセージをやり取りしていない時間の長さをhh:mm:ssの形式で示します。アイドル時間が24時間以上の場合、oldと表示される
Time	ユーザがログインした時刻
Pid	ユーザのプロセスID (CLIユーザがログインすると、ユーザログインプロセスが自動的に実行され、ユーザのアクションが監視されます。)
Type	ユーザのログイン方法を表示します。 • TELは、ユーザがTelnetでデバイスにログインしたことを示します。 • SSHは、ユーザがSSHを使用してデバイスにログインしたことを示します。 • 表示されていない情報は、ユーザがConsoleポート経由でデバイスにログインしたことを示しています。
+	現在の操作ユーザ
Location	この加入者線でログインしたユーザの位置情報(ユーザのIPアドレス)
F	現在の操作ユーザは非同期モードで作業しています

3.1.8 display web menu

Syntax

display web menu

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display web menu コマンドは、Web インタフェースナビゲーションツリーのすべての情報を表示するために使用します。

例

#現在の Web インタフェースナビゲーションツリーに関する情報を表示します。

<AC> display web menu

```
.
|--Dashboard: ID = m_dashboard
|--Monitoring: ID = m_monitoring
|    |--Clients: ID = m_monclients
|    |    |--Clients Info: ID = m_monclients
|    |    |--Access Category Frames: ID = m_acframe
|    |    |--Access Category Bytes: ID = m_acbyte
|    |    |--Total Frames: ID = m_totalframe
|    |    `--Total Bytes: ID = m_totalbyte
|    |--Wireless Networks: ID = m_monwirelessnetworks
|    |    |--Wireless Services: ID = m_monssid
|    |    `--Wireless Services Statistics: ID = m_wsreport
|    |--Access Points: ID = m_monaccesspoints
|    |    |--APs: ID = m_monaps
|    |    |--AP Groups: ID = m_monapgroups
|    |    `--APs Statistics: ID = m_apreports
|    |--RF Monitoring: ID = m_rfmonitoring
|    |    |--RRM: ID = m_monrfoptimization
|    |    `--Spectrum Analysis: ID = m_monitoringspectrumanalysis
|    |--Wireless Security: ID = m_wipssecurity
|    |    `--WIPS: ID = m_wipsdashboard
|    `--Application Monitoring: ID = m_appmonitoring
|        |--Bonjour: ID = m_monbonjour
|        |--Multicast Optimization: ID = m_monitoringmulticast
|        `--Client Proximity Sensor: ID = m_monprobe
```

3.1.9 display web users

Syntax

display web users

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display web users コマンドは、Web ユーザに関する情報を表示するために使用します。

例

#現在の Web ユーザに関する情報を表示します。

<AC> display web users

```
UserID        Name          Type   Language JobCount LoginTime LastOperation
AB2039483271293 Administrator   HTTP   Chinese    3    12:00:23  14:10:05
F09382BA2014AC8 user          HTTPS  English    1    13:05:00  14:11:00
```

表 3-6 display web users コマンドの表示情報の説明

フィールド	説明
UserID	ログインユーザを一意に識別するWebユーザのID番号
Name	Webユーザのログインユーザ名
Type	Webユーザのログインに使用されるプロトコルのタイプ: ● HTTP表現Hypertext Transfer Protocol ● HTTPSは、Secure SocketsベースのHypertext Transfer Protocol を表します。
Language	Webユーザがログインするときに使用する言語: ● Chineseは中国語 ● Englishは英語
JobCount	Webユーザが確立した接続の数
LoginTime	Webユーザのログイン時間
LastOperation	Webユーザの最終操作時間

3.1.10 escape-key

Syntax

escape-key { *key-string* | **default** }

undo escape-key

デフォルト

<Ctrl+C>キーを押して、実行中のタスクを終了します。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

key-string:実行中のタスクを終了させるためのショートカットを定義します。このショートカットには、大文字と小文字を区別する 1 文字のショートカット(文字 「d」 と 「D」 を除く)と、1 文字のショートカットまたはキーの組み合わせに対する ACSII コード(0~127)があります。例えば escape-key 1 を設定すると、Ctrl+A のショートカットが有効になります。escape-key a を設定すると、ショートカットキーは a になります。実行中のタスクを終了するためのショートカットとして設定文字 「d」 および 「D」 が有効になっていない場合、<Ctrl+C>が実際の有効なショートカットになります。実行中のタスクを終了するためのショートカットとして文字 「d」 および 「D」 を使用する必要がある場合は、文字 「d」 および 「D」 に対応する ACSII コードを key-string に設定できます。1 文字のショートカットに対応する ASCII コードは標準の ASCII コードテーブルと一致しています。結合キーに対応する ASCII コードは表 3-7 を参照してください。

default:デフォルトのショートカットに戻ります<Ctrl+C>。

表 3-7 ASCII コードの説明

キー	ASCII コードの値
Ctrl+A	1
Ctrl+B	2
Ctrl+C	3
Ctrl+D	4
Ctrl+E	5
Ctrl+F	6
Ctrl+G	7
Ctrl+H	8
Ctrl+I	9
Ctrl+J	10
Ctrl+K	11
Ctrl+L	12
Ctrl+M	13
Ctrl+N	14
Ctrl+O	15
Ctrl+P	16

キー	ASCII コードの値
Ctrl+Q	17
Ctrl+R	18
Ctrl+S	19
Ctrl+T	20
Ctrl+U	21
Ctrl+V	22
Ctrl+W	23
Ctrl+X	24
Ctrl+Y	25
Ctrl+Z	26
CTRL+ [	27
CTRL+¥	28
CTRL+]	29
CTRL+^	30
CTRL+_	31

説明

escape-key コマンドを使用して、実行中のタスク(例えば ping コマンドなどです)を終了するショートカットを設定します。

undo escape-key コマンドは、デフォルトのショートカットを含め、ショートカットの構成を解除するために使用します。

ユーザは、<Ctrl+C>キーを押して、ping、tracert などの実行中のタスクを終了し、新しいコマンドを入力できます。escape-key が設定されている場合は、<Ctrl+C>の代わりに新しい設定のショートカットを使用できます。コマンドラインでサポートされている<Ctrl+C>終了機能モジュールのソフトウェア実装については、該当するコマンドラインの説明を参照してください。

設定したショートカットキーが 1 文字で、タスクを終了できる場合、ショートカットキーを入力するとコマンドの実行が終了します。終了するタスクがない場合、入力したショートカットは通常の編集文字として機能します。

タスク終了のショートカットとして Device A の User line の下に key-string という 1 文字が設定されている場合、その User line を使用して Device A にログインし、Device A を介して Device B に telnet を入力すると、key-string は Device B で編集文字として入力されます。telnet から Device B までの user line で同じ key-string が構成されている場合、key-string はタスクの実行中にタスクを中止できます。

新しい設定のショートカットは、**display current-configuration |include escape-key** コマンドを使用して表示できます。

設定 escape-key が User line view の下のデフォルトであり、escape-key が User line class view の下に設定されている場合、User line class view の下の設定が有効になります。User line class view で設定されていない場合は、デフォルト値が有効になります。

User line view でこのコマンドを使用して設定したショートカットはすぐに有効になります。User line class view で設定したショートカットは、次回のログイン時に有効になります。

例

#設定 VTY 0 タスクの実行を終了するショートカットは a です。

<AC> system-view
[AC] line vty 0
[AC-line-vty0] escape-key a

検証手順は次のとおりです。

- ping コマンドを使用して、IP アドレス 192.168.1.49 のデバイスが到達可能かどうかを確認し、-c パラメータを使用して、送信する ICMP エコー要求メッセージの数を 20 に指定します。

<AC> ping-c 20 192.168.1.49

```
Ping 192.168.1.49 (192.168.1.49):56 data bytes, press 'a' to break
56 bytes from 192.168.1.49:icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.1.49:icmp_seq=1 ttl=255 time=0.000 ms
```

- a と入力すると、タスクはすぐに終了し、現在の view に戻ります。

```
--- ping statistics for 192.168.1.49 ---
20 packet (s) transmitted, 20 packet (s) received, 0.0% packet loss
round-trip min/avg/max/std-dev =0.000/0.200/1.000/0.400 ms
```

<AC>

3.1.11 free line

Syntax

free line { *number1* | { **aux** | **vty** } *number2* }

View

User view

定義済みユーザロール

network-admin

パラメータ

number1:User line の番号(絶対番号付け)。範囲は 0~64 です。

aux:AUX user line

vty:VTY user line

number2:User line の番号(相対番号付け)。AUXUser line の場合は 0、VTYUser line の場合は 0~63 の範囲。

説明

free line コマンドは、 user line で確立された接続を解放するために使用します。

このコマンドを使用して接続を解放することはできません。

例

#VTY 1 で確立された接続を user line から解放します。

<AC> free line vty 1

```
Are you sure to free line vty1?[Y/N]:y
[OK]
```

3.1.12 free user-interface

Syntax

free user-interface {*number1* **|{aux|vty}** *number2* **}**

View

User view

定義済みユーザロール

network-admin

パラメータ

number1:User line の番号(絶対番号付け)。範囲は 0~64 です。

aux:AUX user line

vty:VTY user line

number2:User line の番号(相対番号付け)。AUXUser line の場合は 0、VTYUser line の場合は 0~63 の範囲。

説明

free user-interface コマンドは、 user line で確立された接続を解放するために使用します。

このコマンドを使用して接続を解放することはできません。

このコマンドの実装は free line に準拠しており、旧バージョンとの互換性のためにのみ予約されています。free line を使用してください。

例

#VTY 1 で確立された接続を user line から解放します。

<AC> free user-interface vty 1

```
Are you sure to free line vty1?[Y/N]:y
[OK]
```

3.1.13 free web users

Syntax

free web users { **all** | **user-id** *user-id* | **user-name** *user-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all:すべての Web ユーザ。

user-id:Web ユーザの ID 番号。15 桁の 16 進数です。ログインに成功した各 Web ユーザには、Web ユーザを一意に識別するユーザ ID が自動的に割り当てられます。

user-name user-name:Web ユーザのユーザ名。1~255 文字の文字列で、大文字と小文字が区別されます。

説明

free web users コマンドは、オンライン Web ユーザを強制的にオフラインにするために使用します。

例

#すべてのオンライン Web ユーザをオフラインにします。

<AC> free web users all

関連コマンド

- display web users

3.1.14 history-command max-size

Syntax

history-command max-size *size-value*

undo history-command max-size

デフォルト

履歴コマンドバッファには、10 個の履歴コマンドを格納できます。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

size-value:保存可能な履歴コマンドの数。0~256 の値をとります。

説明

history-command max-size コマンドは、保存できる現在のユーザのオフライン履歴コマンドの数を設定します。

undo history-command max-size コマンドを使用して、デフォルトの状態を復元します。

各加入者線は 1 つの履歴命令バッファに対応し、バッファに現在のユーザが最近実行した成功した命令を保存し、バッファの容量は保存できる履歴命令の数を決定する。**display history-command** コマンド、上カーソルキー↑、または下カーソルキー↓を使用すると、最近成功した操作をいつでも確認できます。デバイスに同時にログインしているユーザによって、コマンドバッファの履歴が異なります。**display history-command** コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*1 章 CLI*”を参照してください。

ユーザが現在のセッションを終了すると、対応する履歴コマンドバッファに保存されている履歴コマンドが自動的に消去されます。

User line view の下の設定 history-command max-size がデフォルトで、history-command max-size が User line class view の下に設定されている場合、User line view の下の有効な設定値は、User line class view の下の設定になります。User line class view で設定されていない場合は、デフォルト値が有効になります。

このコマンドを使用して設定した、現在の User line の下に保存可能な履歴コマンドの数が、User line view で即座に有効になります。User line class view で設定された保存可能な履歴コマンドの数は、次回のログイン時に有効になります。

例

#設定 VTY 0 ユーザのオフライン履歴コマンドバッファには、最大 20 個の履歴コマンドを格納できます。

<AC> system-view
[AC] line vty 0
[AC-line-vty0] history-command max-size 20

3.1.15 http url allowlist

Syntax

http url allowlist *url*

undo http url allowlist *url*

デフォルト

指定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

url: アクセス可能な Web ページの相対パスを、大文字と小文字を区別しない 1～255 文字で指定します。相対パスは、絶対パスからプロトコル、ドメイン名（IP アドレス）、ポート番号を除外したものです。

説明

http url allowlist コマンドは、HTTP アクセスのための URL を URL 許可リストに追加します。

undo http url allowlist コマンドは、URL 許可リストから URL を削除します。

デバイスの Web インタフェースにログインすると、デバイスは HTTP サーバとして動作します。Web ページ上でタブやリンクをクリックすると、装置はターゲット Web ページに対して自動的に HTTP リクエストを生成します。HTTP リクエストには、通常以下のフィールドが含まれます。

- Referer フィールドーReferer フィールドの値は、HTTP リクエストの送信元アドレスを示すための現在の Web ページの URL です。
- Host フィールドーHost フィールドの値は、ターゲット HTTP サーバのドメイン名（または IP アドレス）とポート番号を示すターゲット Web ページの URL です。

デバイスは Referer と Host フィールド内の IP アドレスが同一かどうかを確認します。IP アドレスが同じ場合、デバイスは HTTP リクエストを正当と見なし、そのリクエストの処理を継続します。IP アドレスが異なる場合、デバイスは HTTP リクエストを不正と見なし、攻撃パケットである可能性があるとしてリクエストを拒否します。

アクセスする Web ページのターゲット URL がドメイン名であるか、ターゲット HTTP サーバがデバイスでない場合、**http url allowlist** コマンドを実行してターゲット URL を URL 許可リストに追加することができます。Host フィールド内の URL が URL 許可リストにある場合、デバイスは Referer フィールドと Host フィールドを確認せず、リクエストを直接正当と見なします。

最大 16 の URL 許可リストエントリがサポートされています。

例

#URL 許可リストエントリを追加します。

<AC> system-view
[AC] http url allowlist /web/frame/login.html

3.1.16 http acl

Syntax

http acl { *advanced-acl-number* | *basic-acl-number* }

undo http acl

デフォルト

すべての IPv4 HTTP クライアントとデバイスに TCP 接続を許可します。

View

System view

定義済みユーザロール

network-admin

パラメータ

advanced-acl-number:拡張 IPv4 ACL を表す番号。範囲は 3000~3999 です。

basic-acl-number:基本 IPv4 ACL を表す番号で、 2000~2999 の範囲の値をとる。

説明

http acl コマンドは、ACL を使用して IPv4 HTTP クライアントとデバイス間の TCP 接続を制限するために使用されます。

undo http acl コマンドを使用して、デフォルトの状態を復元します。

このコマンドを実行すると、デバイスは IPv4 HTTP クライアントとデバイスが新しく確立した TCP 接続のみをフィルタリングし、確立された TCP 接続には影響を与えません。
注意:

- 参照されていない ACL、参照されている ACL が存在しない場合、または参照されている ACL が空の場合は、すべての IPv4 HTTP クライアントとデバイスが TCP 接続を確立できます。
- 参照 ACL が空でない場合、ACL の permit ルールに一致する IPv4 HTTP クライアントだけがデバイスと TCP 接続を確立できます。

このコマンドは、IPv4 HTTP クライアントとデバイスが TCP 接続を確立するのを制限します。接続が確立された後、サービスにアクセスできるかどうかは、サービスの構成によって異なります。例:

- NETCONF over Soap セッション:クライアントがデバイスとセッションを確立できるのは、このコマンドと netconf soap acl コマンドの設定によって IPv4 HTTP クライアントがデバイスにアクセスできるようになっている場合だけです。
- Web 経由のデバイスへのログイン:このコマンドと ip http acl コマンドの設定によって、IPv4 HTTP クライアントがデバイスにアクセスできるようになっている場合にのみ、クライアントはデバイスにアクセスできます。

netconf soap acl コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の”*6 章 NETCONF*”を参照してください。

例

#IPv 4 アドレスが 1.1.1.1 の HTTP クライアントとデバイスのみに TCP 接続を許可するように、HTTP サービスと IPv4 ACL の関連付けを設定します。

<AC> system-view
[AC] acl basic 2001
[AC-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[AC-acl-ipv4-basic-2001] quit
[AC] http acl 2001

関連コマンド

- ip http acl
- netconf soap acl (ネットワーク管理と監視-NETCONF)

3.1.17 https acl

Syntax

https acl { *advanced-acl-number* | *basic-acl-number* }

undo https acl

デフォルト

すべての IPv4 HTTPS クライアントとデバイスに TCP 接続を許可します。

View

System view

定義済みユーザロール

network-admin

パラメータ

advanced-acl-number:拡張 IPv4 ACL を表す番号。範囲は 3000~3999 です。

basic-acl-number:基本 IPv4 ACL を表す番号で、 2000~2999 の範囲の値をとる。

説明

https acl コマンドは、ACL を使用して IPv4 HTTPS クライアントとデバイス間の TCP 接続を制限するために使用されます。

undo https acl コマンドを使用して、デフォルトの状態を復元します。

このコマンドを実行すると、デバイスは IPv4 HTTPS クライアントとデバイスが新しく確立した TCP 接続のみをフィルタリングし、確立された TCP 接続には影響を与えません。注意:

- 参照されていない ACL、参照されている ACL が存在しない場合、または参照されている ACL が空の場合は、すべての IPv4 HTTPS クライアントとデバイスが TCP 接続を確立できます。
- 参照 ACL が空でない場合、ACL の permit ルールに一致する IPv4 HTTPS クライアントだけがデバイスと TCP 接続を確立できます。

このコマンドは、IPv4 HTTPS クライアントとデバイスが TCP 接続を確立するのを制限します。接続が確立された後、サービスにアクセスできるかどうかは、サービスの構成によって異なります。例:

- NETCONF over Soap セッション:クライアントがデバイスとセッションを確立できるのは、このコマンドと netconf soap acl コマンドの設定によって IPv4 HTTPS クライアントがデバイスにアクセスできるようになっている場合だけです。
- Web 経由のデバイスへのログイン:このコマンドと ip https acl コマンドの設定によって、IPv4 HTTPS クライアントがデバイスにアクセスできるようになっている場合にのみ、クライアントはデバイスにアクセスできます。

netconf soap acl コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の”*6 章 NETCONF*”を参照してください。

例

#IPv 4 アドレスが 1.1.1.1 の HTTPS クライアントとデバイスのみが TCP 接続を確立できるように、HTTPS サービスと ACL アソシエーションを設定します。

```
<AC> system-view
[AC] acl basic 2001
[AC-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[AC-acl-ipv4-basic-2001] quit
[AC] https acl 2001
```

関連コマンド

- ip https acl
- netconf soap acl (プログラマブルネットワーク管理コマンドリファレンス/NETCONF)

3.1.18 idle-timeout

Syntax

idle-timeout *minutes [seconds]*

undo idle-timeout

デフォルト

タイムアウト時間は 10 分です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

minutes:タイムアウト時間を分単位で 0~35791 の範囲で指定します。

seconds:タイムアウト時間を秒単位で 0~59 の範囲で指定します。デフォルトは 0 です。

説明

idle-timeout コマンドは、ユーザ接続のタイムアウト時間を設定します。

undo idle-timeout コマンドを使用して、デフォルトの状態を復元します。

ユーザがログインした後、タイムアウト時間内にデバイスとユーザの間にメッセージのやり取りがない場合、タイムアウト時間に達するとデバイスは自動的にユーザを切断します。

タイムアウトが 0 時に設定されている場合は、タイムアウトが発生してもデバイスは自動的にユーザを切断しません。

User line viewの下の設定idle-timeoutがデフォルトで、idle-timeoutがUser line class viewの下に設定されている場合、User line view の下の有効な設定値は、User line class viewの下の設定になります。User line class view で設定されていない場合は、デフォルト値が有効になります。

User line view でこのコマンドを使用して設定した接続タイムアウト時間は即時に有効になります。User line class view で設定された接続タイムアウトは、次回のログイン時に有効になります。

例

#VTY 0 加入者線でのユーザ接続タイムアウトを 1 分 30 秒に設定します。

<AC> system-view
[AC] line vty 0

[AC-line-vty0] idle-timeout 1 30

3.1.19 line

Syntax

line { *first-number1* [*last-number1*] | { **aux** | **vty** } *first-number2* [*last-number2*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

first-number1:最初の User line の番号(絶対番号付け)。範囲は 0~64 です。

last-number1:最後の User line の番号(絶対番号付け)。first-number1 より大きい値を指定してください。

aux:AUX user line。

vty:VTY user line。

first-number2:最初の user line の番号。AUXUser line の場合は 0、VTYUser line の場合は 0~63 の範囲です。

last-number2:最後の User line の番号。AUXUser line ではサポートされていません。VTYUser line では 1~63 の範囲で、first-number2 より大きい値を指定してください。

説明

コマンドラインを使用して、1 つ以上の User line view を表示します。

例

#VTY 0 の User line view に移動します。

<AC> system-view
[AC] line vty 0
[AC-line-vty0]

#VTY 0~63User line view に移動します。

<AC> system-view
[AC] line vty 0 63
[AC-line-vty0-63]

関連コマンド

- line class

3.1.20 line class

Syntax

line class { **aux** | **vty** }

View

System view

定義済みユーザロール

network-admin

パラメータ

aux:AUX ユーザ line class

vty:VTY ユーザ line class

説明

line class コマンドを使用して、User line class view にアクセスします。

User line view の設定は、その User line view に対してのみ有効です。

User line class view での設定の変更は、ユーザが次回ログインしたときに変更された設定値にすぐには反映されません。

line class コマンドを使用して User line class view を表示し、コマンドラインを使用して 1 つまたは複数の User line view を表示します。両方の view をサポートするコマンドの場合:

- User line view の設定は、User line class view の設定よりも優先されます。
- User line view の下の属性がデフォルトとして設定されている場合、User line class view の下で設定されている値が使用されます。User line class view の下のプロパティ構成もデフォルトの場合は、そのプロパティのデフォルト値がそのまま使用されます。

User line class view でサポートされているコマンドは次のとおりです。

- activation-key
- auto-execute command
- authentication-mode
- command accounting
- command authorization
- escape-key
- history-command max-size
- idle-timeout
- protocol inbound
- screen-length
- set authentication password
- shell

- terminal type
- user-role

例

#VTYUser line class view で、ユーザ接続のタイムアウト時間のデフォルト値を 15 分に設定します。

<AC> system-view
[AC] line class vty
[AC-line-class-vty] idle-timeout 15

#AUXUser line class view で、ターミナルセッションのショートカットを<s>に設定します。

<AC> system-view
[AC] line class aux
[AC-line-class-aux] activation-key s
[AC-line-class-aux] quit

- AUXUser line view で、ターミナルセッションのショートカットをデフォルト値(undo activation-key または直接 activation-key 13 を使用して設定できます。)に設定します。

[AC] line aux 0
[AC-line-aux0] undo activation-key

- この時点で有効なショートカットキーは、User line class view の設定で、次のように検証されます。
- ターミナルセッションを終了します。

[AC-line-aux0] return
<AC> quit

- デバイスに再度ログインすると、次のようなメッセージが表示されます。

```
Press ENTER to get started.
```

- この時点で、<Enter>キーが無効になり、User view プロンプトが表示されてターミナルセッションを開始するには、<s>キーを押す必要があります。

<AC>

関連コマンド

- line

3.1.21 lock

Syntax

lock

デフォルト

現在の User line は自動的にはロックされません。

View

User view

定義済みユーザロール

network-admin

説明

lock コマンドは、現在の user line をロックし、ロック解除パスワードを設定して、権限のないユーザがその user line を操作できないようにします。

ユーザが **lock** コマンドを入力すると、パスワードの入力を求められ(パスワードの最大長は 16 文字です。)、パスワードの再入力を求められます。Lock 操作は、同じパスワードを 2 回入力した場合にのみ成功します。加入者線がロックされている場合、ロックを終了してシステムにアクセスするには、ユーザはロック解除パスワードを入力する必要があります。

例

#現在の User line をロックし、ロックを解除します。

<AC> lock

```
Please input password <1 to 16> to lock current line:
Password:
Again:


locked !
```

コマンドライン user line がロックされます。入力して正しいパスワードを入力すると、ロックが解除されます。

```
Password:
```

<AC>

3.1.22 parity

Syntax

parity { **even** | **mark** | **none** | **odd** | **space** }

undo parity

デフォルト

デバイス検証ビットの検証方式は none であり、検証は行わない。

View

User line view

定義済みユーザロール

network-admin

パラメータ

even:偶数の検証を行います。

mark:マークの検証を行います。

none:検証なし。

odd:特異検証を行う。

space:スペースの検証を行います。

説明

parity コマンドは、チェックビットの解析と生成を設定します。

undo parity コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、VTYUser line view ではサポートされていません。

アクセス端末と装置のチェックビットの設定が一致しない場合、正常に通信することはできません。

例

#AUX 加入者線伝送チェックビットを奇数チェックに設定する。

<AC> system-view
[AC] line aux 0
[AC-line-aux0] parity odd

3.1.23 protocol inbound

Syntax

protocol inbound { **all**| **ssh** | **telnet** }

undo protocol inbound

デフォルト

システムはすべてのプロトコルをサポートします。

View

VTY User line view

VTY User line class view

定義済みユーザロール

network-admin

パラメータ

all:Telnet、SSH を含むすべてのプロトコルをサポートします。

ssh:SSH プロトコルをサポートします。

telnet:Telnet プロトコルをサポートします。

説明

protocol inbound コマンドは、 user line でサポートされているプロトコルを指定します。

undo protocol inbound コマンドを使用して、デフォルトの状態を復元します。

User line view では、次回のログイン時にコマンドの設定結果が有効になります。

user line で SSH プロトコルをサポートするように構成する場合は、ユーザの認証方法を scheme に設定する必要があります。設定しないと、protocol inbound ssh コマンドは失敗します。

User line view で、authentication-mode と protocol inbound を関連付けます。

- 両方のコマンドがデフォルトとして設定されている場合、この User line view の下の両方のコマンド設定値は、その User line class view の下の対応する設定を取ります。このクラスの User line class view で適切な設定が行われていない場合は、デフォルト値が使用されます。
- どちらかのコマンドにデフォルト以外の値が設定されている場合、もう一方のコマンドはデフォルト値を使用します。両方のコマンドがデフォルト値以外に設定されている場合は、 user line の設定値が使用されます。

このコマンドを実行できるのは、network-admin または level-15 のユーザロールを持つユーザのみです。他のロールのユーザは、コマンドのアクション権限が付与されている場合でもコマンドを実行できません。

例

#VTY 0 から VTY 4 への加入者線の設定 SSH プロトコルのみサポートされます。

```
<AC> system-view
[AC] line vty 0 4
[AC-line-vty0-4] authentication-mode scheme
[AC-line-vty0-4] protocol inbound ssh
```

#設定 VTY ユーザ line class は SSH プロトコルをサポートし、認証方式は scheme です。また、加入者線 VTY 0 から VTY 4 まではログイン認証を行わず、すべてのプロトコルをサポートするように設定した。

```
<AC> system-view
[AC] line class vty
[AC-line-class-vty] authentication-mode scheme
[AC-line-class-vty] protocol inbound ssh
[AC-line-class-vty] line vty 0 4
[AC-line-vty0-4] authentication-mode none
```

検証手順は次のとおりです。

- Telnet でログインすると、認証なしでログインできます。

<Client> telnet 192.168.1.241

```
Trying 192.168.1.241 ...
Press CTRL+K to abort
Connected to 192.168.1.241 ...
```

<Server>

- 現在使用されている加入者線とユーザに関する情報を表示します。加入者線が line 0 の場合は、その構成の下位の加入者線構成が有効であることを示します。

<Server> display users

```
  Idx  Line     Idle      Time            Pid     Type
+ 50   VTY 0    00:00:00   Jan 17 15:29:27   189     TEL

Following are more details.
VTY 0   :
       Location: 192.168.1.186
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

関連コマンド

- authentication-mode

3.1.24 screen-length

Syntax

screen-length *screen-length*

undo screen-length

デフォルト

1 画面に 24 行のデータが表示されます。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

screen-length:1 画面に表示する行数を 0~512 の範囲で指定します。0 を指定すると、すべての情報が一度に表示されます。つまり、分割表示は行われません。この場合、**screen-length disable** コマンドを実行した場合と同じ結果になります。

説明

screen-length コマンドを使用して、分割画面表示時の 1 画面あたりの表示行数を設定します。

undo screen-length コマンドを使用して、デフォルトの状態を復元します。

このコマンドは 1 画面に表示される行数を設定するが、表示端末が実際に表示する行数は端末の仕様によって決まる。例えば、 screen-length の値を 40 に設定した場合、表示端末の仕様は 24 行であり、一時停止表示時にスペースバーを押すと、デバイスから表示端末に送られる情報は 40 行であるが、現在の画面は 18～40 行目の情報が表示されており、先頭の 17 行目の情報は、 <Page Up>/<Page Down>キーで反転する必要がある。

デバイスは、情報の分割表示をサポートしています。一時停止中にスペースバーを押すと、次の画面に進むことができます。

分割画面表示はデフォルトでオンになっています。

設定 screen-length が User line view の下のデフォルトであり、screen-length が User line class view の下に設定されている場合、User line class view の下の設定が有効になります。User line class view で設定されていない場合は、デフォルト値が有効になります。

User line view でこのコマンドを使用して設定した分割表示情報の行数がすぐに有効になります。User line class view で設定した分割画面表示情報の行数は、次回のログイン時に有効になります。

例

#VTYUser line 分割表示を設定すると、1 画面に 30 行のデータが表示されます。

<AC> system-view
[AC] line vty 0
[AC-line-vty0] screen-length 30

関連コマンド

- screen-length disable (基本構成ガイド/CLI)

3.1.25 send

Syntax

send { **all** | *number1* | { **aux** | **vty** } *number2* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all:すべての加入者線。

number1:User line の番号(絶対番号付け)。範囲は 0~64 です。

aux:AUX user line

vty:VTY user line

number2:User line の番号(相対番号付け)。AUXUser line の場合は 0、VTYUser line の場合は 0~63 の範囲。

説明

send コマンドは、 user line にメッセージを送信するために使用します。

このコマンドを入力して戻ると、メッセージの内容を入力するよう求められます。メッセージの内容を入力するときは、<Enter>キーを押して入力を終了し、<Ctrl+C>キーを押してこの操作を取り消します。

例

#VTY 0 を使用してオンラインになっているユーザがデバイスを再起動したい場合は、「Note please、I will reboot the system in 3 minutes.」というメッセージを VTY 1 に送信します。

<AC> send vty 1

```
Input message、end with Enter;abort with CTRL+C:
Your attention、please.I will reboot the system in 3 minutes.
Send message?[Y/N]:y
```

VTY 1 の user line を使用してログインすると、次のメッセージが表示されます。

[AC]

```
***
***
*** Message from vty0 to vty1
***
Your attention、please.I will reboot the system in 3 minutes.
```

3.1.26 set authentication password

Syntax

set authentication password { **hash** | **simple** } *string*

undo set authentication password

デフォルト

認証パスワードが設定されていません。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

hash:パスワードをハッシュで設定します。

simple:暗号化されたテキストで保存されるパスワードをクリアテキストで設定します。

string:大文字と小文字を区別するパスワード文字列。平文パスワードが 4~16 文字の文字列で、パスワード要素の最小組み合わせタイプが 2 です。ハッシュパスワード 1~110 文字の文字列。

説明

set authentication password コマンドを使用して、認証パスワードを設定します。

undo set authentication password コマンドを使用して、デフォルトの状態を復元します。

クリアテキストまたはハッシュで設定されたパスワードは、ハッシュ化された暗号化テキストとして設定ファイルに保存されます。

set authentication password が User line view の下のデフォルトであり、set authentication password が User line class view の下に設定されている場合、User line class view の下の設定が有効になります。User line class view で設定されていない場合は、デフォルト値が有効になります。

このコマンドを実行できるのは、network-admin または level-15 のユーザロールを持つユーザのみです。他のロールのユーザは、コマンドのアクション権限が付与されている場合でもコマンドを実行できません。

User line view/User line class view では、このコマンドで設定した認証パスワードは、次回デバイスにログインしたときに有効になります。

例

#加入者線 VTY 0 の認証パスワードを hello12345 に設定します。

```
<AC> system-view
[AC] line vty 0
[AC-line-vty0] authentication-mode password
[AC-line-vty0] set authentication password simple hello12345
```

セットアップ後にシステムを終了する場合は、パスワードプロンプトに hello12345 文字列を入力しないとシステムにアクセスできません。

関連する構成

- authentication-mode

3.1.27 shell

Syntax

shell

undo shell

デフォルト

すべての加入者線のターミナルサービス機能がオンになっています。

View

User line view

User line class view

定義済みユーザロール

network-admin

説明

shell コマンドは、現在の user line でターミナルサービスを開始するために使用します。

undo shell コマンドは、現在の user line でターミナルサービスをシャットダウンするために使用します。

undo shell コマンドは、AUXUser line view/AUX user line class view ではサポートされていません。

ユーザは、ログインしている user line で **undo shell** コマンドを使用できません。

デバイスが Telnet/SSH サーバとして機能するとき、**undo shell** コマンドを設定できません。

User line class view で undo shell コマンドを使用してターミナルサービスを閉じた場合、User line view では shell を使用してターミナルサービスを開始できません。

例

#VTY 0~VTY 4 で端末サービスを終了する(ユーザは VTY 0~4 経由でデバイスにログインできなくなる)。

```
<AC> system-view
[AC] line vty 0 4
[AC-line-vty0-4] undo shell
Disable line-vty0-4 、are you sure?[Y/N]:y
```

[AC-line-vty0-4]

3.1.28 speed

Syntax

speed *speed-value*

undo speed

デフォルト

加入者線の伝送速度は 9600 bps。

View

User line view

定義済みユーザロール

network-admin

パラメータ

speed-value:bps 単位の転送レート。非同期シリアルポートの転送速度は、300 bps、600 bps、1200 bps、2400 bps、4800 bps、9600 bps、19200 bps、38400 bps、57600 bps、115200 bps です。非同期シリアルポートの転送速度は、設定時のネットワーク環境に依存します。ネットワーク環境に応じて、非同期シリアルポートの転送速度を設定します。

説明

speed コマンドは、加入者線の転送速度を設定します。

undo speed コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、VTYUser line view ではサポートされていません。

通信を正常に行うには、アクセス端末とデバイスのそれぞれの加入者線の転送速度設定が一致している必要があります。

例

#加入者線 AUX 0 の転送速度を 19200 bps に設定します。

<AC> system-view
[AC] line aux 0
[AC-line-aux0] speed 19200

3.1.29 stopbits

Syntax

stopbits { **1** | **1.5** | **2** }

undo stopbits

デフォルト

ストップビットは 1 ビットである。

View

User line view

定義済みユーザロール

network-admin

パラメータ

1:ストップビットは 1 ビットである。

1.5:ストップビットは 1.5 ビットである。現時点では、デバイスはこのパラメータをサポートしていません。設定後に実際に有効になるのは、コマンドライン stopbits 2 です。

2:ストップビットは 2 ビットである。

説明

stopbits コマンドは、ストップビットの数を設定します。

undo stopbits コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、VTYUser line view ではサポートされていません。

アクセス端末と機器のそれぞれの加入者線下ストップビットの設定は、双方が正常に通信するために一致しなければならない。

例

#AUX 加入者線のストップビットを 1 ビットとする。

<AC> system-view
[AC] line aux 0
[AC-line-aux0] stopbits 1

3.1.30 telnet

Syntax

telnet *remote-host* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* } | **dscp** *dscp-value*] *

View

User view

定義済みユーザロール

network-admin

パラメータ

remote-host:リモートデバイスの IPv 4 アドレスまたはホスト名。ここで、ホスト名は 1~253 文字の文字列で、大文字と小文字は区別されません。文字列には、英字、数字、「-」、「_」 、または 「.」 のみを使用できます。

service-port:リモートデバイスが Telnet サービスを提供する TCP ポート番号。範囲は 0~65535 で、デフォルト値は 23 です。

source:Telnet メッセージの送信元インタフェースまたは送信元 IPv 4 アドレスを指定します。このパラメータが指定されていない場合、デバイスが送信する Telnet メッセージの送信元 IPv 4 アドレスとして、ルーテッドインタフェースのプライマリ IP アドレスが使用されます。

interface *interface-type interface-number*:送信元インタフェースを指定します。送信される Telnet メッセージの送信元 IPv 4 アドレスは、このインタフェースのアドレスです。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。

ip *ip-address*:Telnet メッセージの送信元 IPv 4 アドレスを指定します。

dscp *dscp-value*:Telnet クライアントがサーバ側に送信する Telnet メッセージの DSCP 優先度は、0~63 の範囲で設定され、デフォルト値は 48 です。

説明

telnet コマンドは、Telnet がリモート管理のためにリモートデバイスにログインするために使用します。

ユーザは、<Ctrl+K>キーまたは **quit** コマンドを使用して、この Telnet ログインを中断できます。

このコマンドで指定された送信元 IPv 4 アドレスまたは送信元インタフェースは、現在の Telnet 接続でのみ有効です。

例

#Telnet リモートホスト(IP アドレス 1.1.1.2)にログインし、Telnet メッセージを送信する送信元 IP アドレスを 1.1.1.1 に指定します。

<AC> telnet 1.1.1.2 source ip 1.1.1.1

関連コマンド

- telnet client source

3.1.31 telnet client source

Syntax

telnet client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo telnet client source

デフォルト

Telnet メッセージを送信する送信元 IPv 4 アドレスと送信元インタフェースが指定されておらず、Telnet メッセージの送信元アドレスとして、メッセージルーティングアウトインタフェースのプライマリ IPv 4 アドレスが使用されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface interface-type interface-number:送信元インタフェースを指定します。送信される Telnet メッセージの送信元 IPv 4 アドレスは、このインタフェースのアドレスです。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。

ip *ip-address*:Telnet メッセージを送信する送信元 IPv 4 アドレスを指定します。

説明

telnet client source コマンドは、デバイスが Telnet クライアントとして動作するときに Telnet メッセージを送信する送信元 IPv 4 アドレスまたは送信元インタフェースを指定するために使用します。

undo telnet client source コマンドを使用して、デフォルトの状態を復元します。

このコマンドで指定された送信元 IPv 4 アドレスまたは送信元インタフェースは、すべての Telnet 接続で有効です。

このコマンドと **telnet** コマンドの両方を使用して送信元 IPv 4 アドレスまたは送信元インタフェースを指定する場合は、**telnet** コマンドで指定した送信元 IP アドレスまたは送信元インタフェースを使用します。

例

#デバイスが Telnet クライアントの場合、送信する Telnet メッセージの送信元 IP アドレスを 1.1.1.1 と指定する。

<AC> system-view
[AC] telnet client source ip 1.1.1.1

関連コマンド

- display telnet client configuration

3.1.32 telnet server acl

Syntax

telnet server acl [**mac**] *acl-number*

undo telnet server acl

デフォルト

Telnet クライアントを制限するために ACL は使用されません。

View

System view

定義済みユーザロール

network-admin

パラメータ

mac:レイヤ 2 ACL を指定します。このキーワードを指定しない場合は、IPv4 ACL となります。

acl-number ： ACL を番号で指定します。mac キーワードを指定した場合、この引数の値の範囲は 4000 から 4999 です。mac キーワードを指定しない場合、この引数の値の範囲は 2000 から 3999 です。

説明

telnet server acl コマンドは、ACL (Access Control List、アクセス制御リスト#アクセスセイギョリスト#)を使用して、どの Telnet クライアントがデバイスにアクセスできるかを制限するために使用します。

undo telnet server acl コマンドを使用して、デフォルトの状態を復元します。

ACL 制限 Telnet クライアントを設定する場合:

- ACL が参照されていない場合に、すべてのログインユーザがデバイスにアクセスできるようにする;
- ACL が存在しない場合、または参照 ACL が空の場合、すべてのログインユーザがデバイスにアクセスできないようにします。
- 参照 ACL が空でない場合、ACL 内の permit のユーザのみがデバイスにアクセスでき、他のユーザは Telnet を使用してデバイスにアクセスできないようにデバイスへのアクセスを許可されません。
- このコマンドを複数回使用して Telnet サービスを ACL に関連付けるように設定すると、最新の設定が有効になります。

ACL の詳細な説明は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。

この設定では、新しく確立された Telnet 接続のみがフィルタリングされ、確立された Telnet 接続と操作には影響しません。

例

#アドレスが 1.1.1.1 のユーザだけが Telnet を介してこのデバイスにアクセスできます。

<AC> system-view

```
[AC] acl basic 2001
[AC-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[AC-acl-ipv4-basic-2001] quit
[AC] telnet server acl 2001
```

3.1.33 telnet server dscp

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

デフォルト

Telnet サーバが Telnet メッセージを送信する DSCP の優先度は 48 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value:Telnet メッセージの DSCP 優先度。範囲は 0~63 です。

説明

telnet server dscp コマンドを使用して、Telnet サーバが Telnet メッセージを送信する DSCP プライオリティを設定します。

undo telnet server dscp コマンドを使用して、デフォルトの状態を復元します。

DSCP は IP メッセージ中の ToS フィールドを持ち、メッセージ自体の優先順位を表し、メッセージ転送の優先度を決定する。

例

#Telnet サーバがメッセージを送信する DSCP プライオリティを 30 に設定します。

```
<AC> system-view
[AC] telnet server dscp 30
```

3.1.34 telnet server enable

Syntax

telnet server enable

undo telnet server enable

デフォルト

Telnet サービスが停止しています。

View

System view

定義済みユーザロール

network-admin

説明

telnet server enable コマンドは、Telnet サービスを開始するために使用します。

undo telnet server enable コマンドは、Telnet サービスを停止するために使用します。

ネットワーク管理者が Telnet プロトコルを使用してデバイスにログインできるようにするには、Telnet サービスを有効にする必要があります。

例

#Telnet サービスを有効にします。

<AC> system-view
[AC] telnet server enable

3.1.35 telnet server port

Syntax

telnet server port *port-number*

undo telnet server port

デフォルト

23

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: ポート番号を指定します。値は 23 または 1025 から 65535 の範囲です。

説明

IPv4 Telnet サービスポート番号を指定するには、**telnet server port** を使用します。

デフォルトに戻すには、**undo telnet server port** を使用します。

このコマンドは、IPv4 Telnet サーバへの既存の Telnet 接続をすべて終了します。Telnet サービスを使用するには、ユーザは Telnet 接続を再確立する必要があります。

例

telnet サービスのポート番号を 1025 に変更します。

<AC> system-view

[AC] telnet server port 1025

3.1.36 terminal type

Syntax

terminal type { **ansi** | **vt100** }

undo terminal type

デフォルト

端末の表示タイプは ANSI です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

ansi:端末表示タイプは ANSI タイプです。

vt100:端末の表示タイプは VT100 タイプです。

説明

terminal type コマンドは、現在の user line の下の端末の表示タイプを設定します。

undo terminal type コマンドを使用して、デフォルトの状態を復元します。

デバイスは、ANSI と VT100 の両方の端末ディスプレイタイプをサポートします。デバイスの端末タイプとクライアント(ハイパーターミナルや Telnet クライアントなど)の端末タイプが一致しない場合、または両方が ANSI に設定されていて、現在の編集行の合計文字数が 80 文字を超える場合、クライアントでカーソルがずれて端末画面が正しく表示されないことがあります。両端を VT100 に設定することをお勧めします。

User line view での設定がデフォルトの場合、User line class view での設定値が使用されます。User line class view の下のプロパティ構成もデフォルトの場合、その user line コンフィギュレーションのデフォルト値が使用されます。

User line view/User line class view で設定した端末表示タイプは、次回ログイン時に有効になります。

例

#端末の表示タイプを VT100 に設定します。

<AC> system-view
[AC] line vty 0
[AC-line-vty0] terminal type vt100

3.1.37 user-interface

Syntax

user-interface { *first-number1* [*last-number1*] | { **aux** | **vty** } *first-number2* [*last-number2*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

first-number1:最初の User line の番号(絶対番号付け)。範囲は 0~64 です。

last-number1:最後の User line の番号(絶対番号付け)。first-number1 より大きい値を指定してください。

aux:AUX user line。

vty:VTY user line。

first-number2:最初の User line の番号(相対番号付け)。AUXUser line の場合は 0、VTYUser line の場合は 0~63 の範囲です。

last-number2:最後の User line の番号(相対番号付け)。AUXUser line ではサポートされていません。VTYUser line では 1~63 の値をとります。このパラメータは first-number2 より大きい値をとる必要があります。

説明

user-interface コマンドを使用すると、1 つまたは複数の User line view にアクセスできます。

このコマンドの実装は line に準拠しており、旧バージョンとの互換性のために予約されています。line を使用してください。

設定のために User line view を入力すると、設定はその User view に対してのみ有効になります。

複数の User line view を設定すると、その設定はそれらの User view に対して有効になります。

例

#AUX 0 の User line view に移動します。

<AC> system-view
[AC] user-interface aux 0
[AC-line-aux0]

#VTY 0~4User line view に移動します。

<AC> system-view
[AC] user-interface vty 0 4
[AC-line-vty0-4]

関連コマンド

- user-interface class

3.1.38 user-interface class

Syntax

user-interface class { **aux** | **vty** }

View

System view

定義済みユーザロール

network-admin

パラメータ

aux:AUX ユーザ line class。

vty:VTY ユーザ line class。

説明

user-interface class コマンドを使用して、User line class view にアクセスします。

このコマンドの実装は line class に準拠しており、旧バージョンとの互換性のためにのみ予約されています。line class を使用してください。

User line view の設定は、その User line view に対してのみ有効です。

User line class view での設定の変更は、ユーザが次回ログインしたときに変更された設定値にすぐには反映されません。

user-interface class コマンドは user line class view に、**user-interface** コマンドは 1 つまたは複数の User line view に入ります。両方の view をサポートするコマンドの場合:

- User line view の設定は、User line class view の設定よりも優先されます。
- User line view の下の属性がデフォルトとして設定されている場合、User line class view の下で設定されている値が使用されます。User line class view の下のプロパテ

ィ構成もデフォルトの場合は、そのプロパティのデフォルト値がそのまま使用されます。

User line class view でサポートされているコマンドは次のとおりです。

- activation-key
- auto-execute command
- authentication-mode
- command accounting
- command authorization
- escape-key
- history-command max-size
- idle-timeout
- protocol inbound
- screen-length
- set authentication password
- shell
- terminal type
- user-role

例

#VTYUser line class view で、ユーザ接続のタイムアウト時間のデフォルト値を 15 分に設定します。

<AC> system-view
[AC] user-interface class vty
[AC-line-class-vty] idle-timeout 15

#AUXUser line class view で、ターミナルセッションのショートカットを<s>に設定します。

<AC> system-view
[AC] user-interface class aux
[AC-line-class-aux] activation-key s
[AC-line-class-aux] quit

- AUX User line view で、ターミナルセッションのショートカットをデフォルト値(undo activation-key または直接 activation-key 13 を使用して設定できます。)に設定します。

[AC] user-interface aux 0
[AC-line-aux0] undo activation-key

- この時点で有効なショートカットキーは、User line class view の設定で、次のように検証されます。
- ターミナルセッションを終了します。

[AC-line-aux0] return
<AC> quit

- デバイスに再度ログインすると、次のようなメッセージが表示されます。

```
Press ENTER to get started.
```

- この時点で、<Enter>キーが無効になり、User view プロンプトが表示されてターミナルセッションを開始するには、<s>キーを押す必要があります。

<AC>

関連コマンド

user-interface

3.1.39 user-role

Syntax

user-role *role-name*

undo user-role [*role-name*]

デフォルト

Console からシステムにログインするデフォルトのユーザロールは **network-admin** です。別のインタフェースからシステムにログインするためのデフォルトのユーザロールは network-operator です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

role-name:ユーザロール名。1~63 文字の文字列で、大文字と小文字が区別されます。は、network-admin、network-operator、level-0~level-15 などのシステム定義のロール名、またはカスタムのユーザロール名です。このパラメータを指定しない場合は、デフォルトに戻ります。システム定義ロール security-audit および guest-manager は、user line/User line class view での設定をサポートしていません。

説明

user-role コマンドは、現在の user line からシステムにログインするユーザロールを設定します。

undo user-role コマンドを使用して、ユーザロールを削除するか、デフォルトの状態に戻します。

このコマンドで設定したユーザロールは、次回デバイスにログインしたときに有効になります。

User line view の下の属性がデフォルトとして設定されている場合、その User line class view で設定されているユーザロールが使用されます。User line class view で設定されて

いるユーザロールもデフォルトである場合、その user line レベルのデフォルト値がそのまま使用されます。

このコマンドを実行できるのは、network-admin または level-15 のユーザロールを持つユーザのみです。他のロールのユーザは、コマンドのアクション権限が付与されている場合でもコマンドを実行できません。

このコマンドを複数回実行することで、最大 64 個のユーザロールを設定できます。ユーザがログインしたときに持つ権限は、これらのロール権限の集合です。

ユーザロールの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。

例

#AUX user line からシステムにログインするユーザロールを network-admin に設定します。

<AC> system-view
[AC] line aux 0
[AC-line-aux0] user-role network-admin

3.1.40 web idle-timeout

Syntax

web idle-timeout *idle-time*

undo web idle-timeout

デフォルト

Web アイドルタイムアウトは 10 分です。

View

System view

定義済みユーザロール

network-admin

パラメータ

idle-time:Web アイドルタイムアウト時間。1~999 の値を分単位で指定できます。

説明

web idle-timeout コマンドは、Web アイドルタイムアウト時間を設定します。

undo web idle-timeout コマンドを使用して、デフォルトの状態を復元します。

Web ユーザがマウスのクリックやキーボード操作(マウスを動かすだけでは、ユーザのオフライン時間は長くなりません)を含めて idle-time 内の Web ページを操作しない場合、そのユーザの Web リンクは強制的に切断され、ユーザはオフラインになります。これに

より、ユーザがログイン端末から離れている間に、不正なユーザがデバイスを設定することを極力避ける。

Web ラインのアイドルタイムアウト時間を変更すると、アクセスしているユーザに影響することに注意してください。

例

Web アイドルタイムアウトを 100 分に設定します。

<AC> system-view
[AC] web idle-timeout 100

目次

このセクションのページは **2-x-x** です。

4 章 FTP 4-1
4.1 FTP サーバの設定コマンド 4-1
4.1.1 display ftp-server 4-1
4.1.2 display ftp-user 4-2
4.1.3 free ftp user 4-3
4.1.4 free ftp user-ip 4-3
4.1.5 ftp server acl 4-4
4.1.6 ftp server dscp 4-5
4.1.7 ftp server enable 4-6
4.1.8 ftp timeout 4-7
4.2 FTP クライアントの設定コマンド 4-8
4.2.1 ? 4-8
4.2.2 ascii 4-9
4.2.3 binary 4-10
4.2.4 bye 4-10
4.2.5 cd 4-11
4.2.6 cdup 4-12
4.2.7 close 4-13
4.2.8 debug 4-14
4.2.9 delete 4-14
4.2.10 dir 4-15
4.2.11 disconnect 4-16
4.2.12 display ftp client source 4-17
4.2.13 ftp 4-18
4.2.14 ftp client source 4-20
4.2.15 get 4-21
4.2.16 help 4-22
4.2.17 lcd 4-23
4.2.18 ls 4-24
4.2.19 mkdir 4-26
4.2.20 newer 4-26
4.2.21 open 4-27
4.2.22 passive 4-28
4.2.23 put 4-29
4.2.24 pwd 4-30
4.2.25 quit 4-31

4.2.26 rhelp 4-31
4.2.27 rmdir 4-33
4.2.28 user 4-34
4.2.29 verbose 4-35

4章 FTP

4.1 FTPサーバの設定コマンド

4.1.1 display ftp-server

Syntax

display ftp-server

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display ftp-server コマンドを使用して、デバイスが FTP サーバとして動作しているときの設定と動作を表示します。

例

#FTP サーバの設定と動作を表示します。

<Sysname> display ftp-server

```
FTP server is running.
User count:1
Idle-timeout timer (in minutes):30
```

表 4-1 display ftp-server コマンドの表示情報の説明

フィールド	説明
FTP server is running	FTPサーバ機能が実行中です
User count	現在ログインしているユーザの数
Idle-timeout timer (in minutes)	FTP接続が自動的に切断されるまでのアイドル時間。この時間内にFTPクライアントとFTPサーバ間のメッセージのやり取りがなければ、FTP接続は切断されます。

関連コマンド

- **ftp server enable**
- **ftp timeout**

4.1.2 display ftp-user

Syntax

display ftp-user

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display ftp-user コマンドを使用して、FTP ユーザの詳細を表示します。

例

#FTP ユーザの詳細を表示します。

<Sysname> display ftp-user

```
UserName     HostIP           Port     HomeDir
root        192.168.20.184     46539    flash:
```

ログインユーザ名の長さが 10 桁を超える場合は、行が折り返され、左揃えで表示されます。ログインしているユーザの IP アドレスの長さが 15 ビットを超えると、改行して左揃えで表示される;ユーザのルートパスの長さが 37 ビットを超える場合は、行が折り返され、左揃えで表示されます。形状:

<Sysname> display ftp-user

```
UserName     HostIP           Port     HomeDir
user2       2000:2000:2000:    1499     flash:/user2
           2000:2000:2000:
           2000:2000
administra   100.100.100.100    10001    flash:/123456789/123456789/123456789/
tor                                 123456789/123456789/123456789/1234567
                                   89/123456789
```

表 4-2 display ftp-user コマンドの表示情報の説明

フィールド	説明
UserName	現在ログインしているFTPユーザ名
HostIP	現在ログインしているFTPユーザのIPアドレス
Port	現在ログインしているFTPユーザが使用しているポート番号

フィールド	説明
HomeDir	現在ログインしているFTPユーザの認証パス

4.1.3 free ftp user

Syntax

free ftp user *username*

View

User view

定義済みユーザロール

network-admin

パラメータ

username:ユーザ名。**display ftp-user** コマンドを使用して、現在の FTP ユーザに関する情報を表示できます。

説明

free ftp user コマンドは、ユーザ名を使用して確立された FTP 接続の解放を強制するために使用します。

例

#ユーザ名 ftpuser で確立された FTP 接続を強制的に解放します。

<Sysname> free ftp user ftpuser

```
Are you sure to free FTP connection?[Y/N]:y
```

<Sysname>

4.1.4 free ftp user-ip

Syntax

free ftp user-ip *ip-address* [**port** *port*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip-address:解放されるべき FTP 接続のソース IP。display ftp-user コマンドを使用して、現在の FTP 接続のソース IP を表示できます。

port *port*:解放する FTP 接続の送信元ポート。port は送信元ポートのポート番号です。**display ftp-user** コマンドを使用して、現在の FTP 接続の送信元ポートを表示できます。

説明

free ftp user-ip コマンドは、IPv 4 アドレスを使用して確立された FTP 接続の解放を強制するために使用します。

例

#IP アドレス 192.168.20.184 で確立された FTP 接続を強制的に解放します。

<Sysname> free ftp user-ip 192.168.20.184

```
Are you sure to free FTP connection?[Y/N]:y
```

<Sysname>

4.1.5 ftp server acl

Syntax

ftp server acl { *advanced-acl-number* | *basic-acl-number*}

undo ftp server acl

デフォルト

FTP クライアントを制限するために ACL は使用されません。

View

System view

定義済みユーザロール

network-admin

パラメータ

advanced-acl-number:拡張 IPv4 ACL を表す番号。範囲は 3000~3999 です。

basic-acl-number:ベース IPv4 ACL を表す番号。範囲は 2000~2999.

説明

ftp server acl コマンドは、ACL を使用して、デバイスにアクセスできる FTP クライアントを制限するために使用します。

undo ftp server acl コマンドを使用して、デフォルトの状態を復元します。

FTP サービスを ACL に関連付けると、特定の FTP クライアントからの FTP 要求メッセージがフィルタリングされ、ACL フィルタリングルールに準拠した FTP クライアントのみがデバイスにアクセスできるようになります。

FTP クライアントを制限するために ACL を設定して下さい:

- ACL が参照されていない場合、すべての FTP クライアントがデバイスにアクセスできるようにします。
- 参照 ACL が存在しないか空の場合、すべての FTP クライアントがデバイスにアクセスできないようにします。
- 参照 ACL が空でない場合、ACL 内の permit のユーザのみがデバイスにアクセスでき、他のユーザはデバイスにアクセスできないようにすることで、デバイスへの不正なユーザアクセスを回避できます。
- このコマンドを複数回使用して、ACL に関連付けられた FTP サービスを設定すると、最新の設定が有効になります。

ACL の詳細な説明は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。

この設定では、新しく確立された FTP 接続のみがフィルタリングされ、確立された FTP 接続と操作には影響しません。

例

#FTP サービスが ACL に関連付けられ、FTP クライアント(1.1.1.1)のみが FTP 経由でこのデバイスにアクセスできるように設定します。

<Sysname> system-view

[Sysname] acl basic 2001

[Sysname-acl-ipv4-basic-2001] rule 0 permit source 1.1.1.1 0

[Sysname-acl-ipv4-basic-2001] rule 1 deny source any

[Sysname-acl-ipv4-basic-2001] quit

[Sysname] ftp server acl 2001

4.1.6 ftp server dscp

Syntax

ftp server dscp *dscp-value*

undo ftp server dscp

デフォルト

FTP サーバが送信する FTP メッセージの DSCP 優先度は 0 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value:デバイスが送信する FTP メッセージの DSCP 優先度を 0~63 の範囲で指定します。

説明

ftp server dscp コマンドを使用して、FTP サーバから送信される FTP メッセージの DSCP 優先順位を設定します。

undo ftp server dscp コマンドを使用して、デフォルトの状態を復元します。

DSCP は IP メッセージ中の ToS フィールドを持ち、メッセージ自体の優先順位を表し、メッセージ転送の優先度を決定する。

例

#FTP サーバが送信する FTP メッセージの DSCP 優先順位を 30 に設定します。

<Sysname> system-view

[Sysname] ftp server dscp 30

4.1.7 ftp server enable

Syntax

ftp server enable

undo ftp server enable

デフォルト

FTP サーバ機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

ftp server enable コマンドは、デバイスの FTP サーバ機能をオンにして、FTP ユーザがログインできるようにします。

undo ftp server enable コマンドは、デバイスの FTP サーバ機能をシャットダウンするために使用されます。

例

#デバイスの FTP サーバ機能をオンにします。

<Sysname> system-view

[Sysname] ftp server enable

4.1.8 ftp timeout

Syntax

ftp timeout *minute*

undo ftp timeout

デフォルト

FTP 接続が自動的に切断されるまでのアイドル時間は 30 分です。

View

System view

定義済みユーザロール

network-admin

パラメータ

minute:FTP 接続が自動的に切断されるまでのアイドル時間。1~35791 の値を分単位で指定できます。

説明

ftp timeout コマンドは、FTP 接続が自動的に切断されるまでのアイドル時間を設定します。

undo ftp timeout コマンドを使用して、デフォルトの状態を復元します。

設定された接続アイドル時間が経過しても、FTP サーバとクライアントが情報をやり取りしない場合、FTP サーバは接続が失敗したと判断して接続を解除し、システムリソースが継続的に消費され、他の FTP ユーザのログインに影響が及ぶのを防ぎます。

例

#FTP 接続が自動的に切断されるまでのアイドル時間を 36 分に設定します。

<Sysname> system-view
[Sysname] ftp timeout 36

4.2 FTPクライアントの設定コマンド

🕮 **メモ：**

- FTP ユーザが FTP クライアント設定コマンドを実行するには、FTP サーバでユーザの認可設定を行う必要があります。認可された操作には、作業ディレクトリ内のファイルの表示、ファイルの読み取り/ダウンロード/アップロード/名前変更/削除、およびディレクトリの作成が含まれます。
- このセクションの FTP クライアントコマンドはデバイスによってサポートされていますが、正常に実行できるかどうかは FTP サーバによって異なります。
- このセクションの例の出力は、FTP サーバタイプによって異なります。

4.2.1 ?

Syntax

***?**[command-name]*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

command-name:コマンド名。

説明

?コマンドを使用して、すべての FTP クライアントでサポートされているコマンドの名前を表示します。

?command-name コマンドは、指定したコマンドのヘルプ情報を表示します。

FTP クライアントビューの下で、か。コマンドは、help コマンドと同じです。

例

#FTP クライアントでサポートされているすべてのコマンドの名前を表示します。

ftp>?

```
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
```

```
bye           disconnect     open          rhelp         user
cd            get            passive       rename        verbose
cdup          help           put           reset         ?
close         lcd            pwd           restart
```

#dir コマンドのヘルプを表示する

ftp>?dir

```
dir            list contents of remote directory
```

関連コマンド

- **help**

4.2.2 ascii

Syntax

ascii

デフォルト

ファイル転送モードはバイナリモードです。

View

FTP client view

定義済みユーザロール

network-admin

説明

ascii コマンドは、ファイル転送のモードを ASCII モードに設定します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

デバイスが FTP サーバとして機能する場合、使用される転送モードは FTP クライアントによって決定されます。デバイスが FTP クライアントである場合、使用される転送モードはコマンドラインから変更できます。デフォルトはバイナリモードです。

非テキストファイルを転送するにはバイナリモードを使用し、テキストファイルを転送するには ASCII モードを使用します。

例

#データ転送のモードを ASCII に設定します。

ftp>ascii

```
200 TYPE is now ASCII
```

関連コマンド

- **binary**

4.2.3 binary

Syntax

binary

デフォルト

ファイル転送モードはバイナリモードです。

View

FTP client view

定義済みユーザロール

network-admin

説明

binary コマンドは、ファイル転送のモードをバイナリモード(ストリームモードとも呼ばれます)に設定します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

デバイスが FTP サーバとして機能する場合、使用される転送モードは FTP クライアントによって決定されます。デバイスが FTP クライアントである場合、使用される転送モードはコマンドラインから変更できます。デフォルトはバイナリモードです。

非テキストファイルを転送するにはバイナリモードを使用し、テキストファイルを転送するには ASCII モードを使用します。

例

#ファイル転送タイプをバイナリモードに設定します。

ftp>binary

```
200 TYPE is now 8-bit binary
```

関連コマンド

- **ascii**

4.2.4 bye

Syntax

bye

View

FTP client view

定義済みユーザロール

network-admin

説明

bye コマンドを使用して FTP サーバから切断し、User view に戻ります。デバイスが FTP サーバに接続されていない場合は、User view に直接戻ります。

例

#FTP サーバへの接続を終了し、User view に戻ります。

ftp>bye

```
221-Goodbye.You uploaded 2 and downloaded 2 kbytes.
221 Logout.
```

<Sysname>

関連コマンド

- **quit**

4.2.5 cd

Syntax

cd { *directory* | **..** | */* }

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory:ターゲットワークディレクトリを指定します。指定した作業ディレクトリが存在しない場合は、cd directory を実行しても現在の作業ディレクトリは変更されません。

..:cdup と同様の機能を持つ上位ディレクトリを返します。現在の作業ディレクトリがすでに FTP ルートである場合は、cd ..を実行しても現在の作業ディレクトリは変更されません。

/:FTP ルートディレクトリを返します。

説明

cd コマンドは、FTP サーバ上の作業ディレクトリを切り替えます。つまり、FTP サーバ上の別のディレクトリにアクセスします。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

ユーザがアクセスできるディレクトリは、FTP サーバがユーザに許可したディレクトリのみです。

例

#現在の作業ディレクトリの logfile サブディレクトリに作業ディレクトリを切り替えます。

ftp>cd logfile

```
250 OK.Current directory is /logfile
```

#FTP ルートディレクトリの folder サブディレクトリの下にワーキングディレクトリを切り替えて下さい。

ftp>cd /folder

```
250 OK.Current directory is /folder
```

#現在の作業ディレクトリの上位ディレクトリに作業ディレクトリを切り替えます。

ftp>cd ..

```
250 OK.Current directory is /
```

#FTP ルートディレクトリの下にワーキングディレクトリを切り替えて下さい。

ftp>cd/

```
250 OK.Current directory is /
```

関連コマンド

- **cdup**
- **pwd**

4.2.6 cdup

Syntax

cdup

View

FTP client view

定義済みユーザロール

network-admin

説明

cdup コマンドを使用して、FTP サーバの現在の作業ディレクトリを終了し、FTP サーバの上位ディレクトリに戻ります。現在の作業ディレクトリがすでに FTP ルートである場合は、このコマンドを実行しても、現在の作業ディレクトリは変更されません。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

例

#ワーキングディレクトリを 1 つ上のディレクトリに変更します。

ftp>pwd

```
257 "/ftp/subdir" is your current location
```

ftp>cdup

```
250 OK.Current directory is /ftp
```

ftp>pwd

```
257 "/ftp" is your current location
```

関連コマンド

- **cd**
- **pwd**

4.2.7 close

Syntax

close

View

FTP client view

定義済みユーザロール

network-admin

説明

close コマンドは、FTP クライアントビューを終了せずに FTP サーバから切断するために使用します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

例

#FTP サーバから切断し、FTP クライアントビューを維持します。

ftp>close

```
221-Goodbye.You uploaded 0 and downloaded 0 kbytes.
221 Logout.
```

ftp>

関連コマンド

- **disconnect**

4.2.8 debug

Syntax

debug

デフォルト

FTP クライアントデバッグメッセージスイッチがオフになっています。

View

FTP client view

定義済み**ユーザロール**

network-admin

説明

debug コマンドは、FTP クライアントデバッグ情報のスイッチ状態を切り替えるために使用します。

このコマンドを繰り返して、FTP クライアントのデバッグ情報スイッチをオンまたはオフにします。

例

#FTP クライアントデバッグメッセージのスイッチ状態を切り替えます。

ftp>debug

```
Debugging on (debug=1).
```

ftp>debug

```
Debugging off (debug=0).
```

4.2.9 delete

Syntax

delete *remotefile*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile:FTP サーバ上のファイルのファイル名。

説明

delete コマンドは、FTP サーバ上のファイルを完全に削除するために使用します。

 注意

使用中のファイルを誤って削除しないように、このコマンドを実行する前に、指定したファイルが使用されないことを確認してください。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

この操作を実行するには、ユーザに削除権限が必要です。

例

#ファイル b.txt を削除します。

ftp>delete b.txt

```
250 Deleted b.txt
```

4.2.10 dir

Syntax

dir *[remotefile [localfile]]*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile:表示する FTP サーバ上のディレクトリまたはファイル名。

localfile:クエリ情報を保存するローカルファイルの名前。

説明

dir コマンドを使用して、FTP サーバの作業ディレクトリにあるすべてのサブディレクトリとファイルの詳細を表示します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

dir remotefile コマンドを使用して、FTP サーバ上のディレクトリまたはファイルの詳細を表示します。

dir remotefile localfile コマンドは、FTP サーバ上のディレクトリまたはファイルの詳細を localfile という名前のローカルファイルに保存します。

FTP クライアントビューでは、**dir** コマンドは **ls** コマンドと同じです。

例

#現在の FTP サーバの作業ディレクトリにあるすべてのフォルダとファイルの情報を表示します。

ftp>dir

```
150 Connecting to port 50201
-rwxr-xr-x1 001481 Jul7 15:36 a.txt
drwxr-xr-x2 008192 Jul2 14:33 diagfile
drwxr-xr-x3 008192 Jul7 15:21 ftp
drwxr-xr-x2 008192 Jul5 09:15 logfile
drwxr-xr-x2 008192 Jul2 14:33 seclog
-rwxr-xr-x1 0040808448 Jul2 14:33 system-a1801.bin
-rwxr-xr-x1 003050 Jul7 12:26 startup.cfg
-rwxr-xr-x1 0054674 Jul4 09:24 startup.mdb
-rwxr-xr-x1 001481 Jul7 12:34 x.cfg
226 9 matches total
```

#ファイル a.txt のクエリ結果を s.txt ファイルに保存します。

ftp>dir a.txt s.txt

```
output to local-file:s.txt?[Y/N] y
150 Connecting to port 50203
226-Glob:a.txt
```

s.txt ファイルの内容を確認します。

ftp>bye

```
221-Goodbye.You uploaded 0 and downloaded 2 kbytes.
221 Logout.
<Sysname> more s.txt
-rwxr-xr-x1 001481 Jul7 12:34 a.txt
```

関連コマンド

- **ls**

4.2.11 disconnect

Syntax

disconnect

View

FTP client view

定義済みユーザロール

network-admin

説明

disconnect コマンドは、FTP クライアントビューを終了せずに FTP サーバから切断するために使用します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

例

#FTP サーバから切断して、FTP クライアントビューを維持します。

ftp>disconnect

```
221-Goodbye.You uploaded 0 and downloaded 0 kbytes.
221 Logout.
```

ftp>

関連コマンド

- **close**

4.2.12 display ftp client source

Syntax

display ftp client source

View

すべてのビュー

定義済みユーザロール

network-admin

network-operator

説明

display ftp client source コマンドを使用して、デバイスが FTP クライアントである場合の送信元アドレスの設定を表示します。

例

#デバイスが FTP クライアントである場合の送信元アドレスの設定を表示します。

<Sysname> display ftp client source

```
The source IP address of the FTP client is 1.1.1.1.
```

4.2.13 ftp

Syntax

ftp [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* } | **-d**] *]

View

User view

定義済みユーザロール

network-admin

パラメータ

ftp-server:FTP サーバのホスト名または IP アドレス。ここで、ホスト名は 1~253 文字の文字列で、大文字と小文字は区別されません。文字列には、英字、数字、「-」 、「_」 、または 「.」 のみを使用できます。

service-port:リモートデバイスが FTP サービスを提供する TCP ポート番号。範囲は 0~65535 で、デフォルト値は 21 です。

dscp *dscp-value*:デバイスが送信する FTP メッセージに含まれる DSCP の優先度を 0~63 の範囲で指定します。デフォルトは 0 です。

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }:FTP 接続の確立に使用する送信元アドレスを指定します。ここで、

- **interface** interface-type interface-number:送信元インタフェースのインタフェースタイプとインタフェース番号を示します。FTP プロトコル・メッセージを送信する場合、デバイスはこのインタフェースで設定されたプライマリ IP アドレスを送信元アドレスとして使用します。送信元インタフェースにプライマリアドレスが設定されていない場合は、接続を確立できません。
- **ip** source-ip-address:送信元 IP アドレス。FTP プロトコル・メッセージを送信すると、デバイスはその IP アドレスを送信元アドレスとして使用します。このアドレスは、デバイスに設定されている IP アドレスでなければ接続できません。

-d:FTP クライアントのデバッグ情報スイッチをオンにします。

説明

ftp コマンドを使用して FTP サーバにログインし､FTP クライアントビューに入ります。

このコマンドは、IPv 4 グループネットワーク環境でのみ使用できます。

パラメータを指定しない場合は、FTP クライアントビューのみが表示され、FTP サーバにログインしません。

パラメータを指定すると、FTP サーバにログインするためのユーザ名とパスワードの入力を求めるプロンプトが表示されます。ユーザ名とパスワードが正しい場合、ログインは成功し、FTP クライアントの表示に進みます。それ以外の場合、ログインは失敗します。

例

#FTP モードを使用して、現在のデバイス Sysname からデバイス FTP Server (IP アドレスは 192.168.0.211 です。)にログインし、FTP 送信メッセージの送信元 IP アドレスは 192.168.0.212 です。

<Sysname> ftp 192.168.0.211 source ip 192.168.0.212

```
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.0.211:(none)):abc
331 Give me your password、please
Password:
230 Logged in successfully
Remote system type is MSDOS.
```

ftp>

#FTP を使用して、現在のデバイスから FTP Server (IP アドレス 192.168.0.211)にログインし、FTP クライアントのデバッグ情報スイッチをオンにします。

<Sysname> ftp 192.168.0.211–d

```
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 FTP service ready.
User (192.168.0.211:(none)):abc
*Feb 10 09:02:24:139 2020 Sysname FTPC/7/EVENT:PAM initialization result:0.
*Feb 10 09:02:24:150 2020 Sysname FTPC/7/EVENT:PAM:Sent a start-accounting
request.Result:0.
*Feb 10 09:02:24:860 2020 Sysname FTPC/7/COMMAND:USER abc
331 Password required for abc.
Password:
*Feb 10 09:02:25:575 2020 Sysname FTPC/7/COMMAND:PASS XXXX
230 User logged in.
215 UNIX Type:L 8
Remote system type is UNIX.
Using binary mode to transfer files.
```

ftp>*Feb 10 09:02:25:640 2020 SIMWARE FTPC/7/COMMAND:SYST

ftp>

表 4-3 ftp ftp-server -d コマンドの表示情報の説明

フィールド	説明
Failed to create a socket.Reason:error-info.	error-infoが原因でSocketの作成に失敗しました
Failed to bind address ip-address.Reason:error-info.	バインドアドレスip-addressがerror-infoで失敗しました

フィールド	説明
Failed to connect to server.Reason:error-info.	error-infoのため、サーバへの接続に失敗しました
Failed to set socket attribute.Reason:error-info.	Socketプロパティの設定がerror-infoで失敗しました
Wrong address family type:number.	間違ったアドレスファミリタイプnumber
Failed to obtain socket name.Reason:error-info.	error-infoのため、Socket名の取得に失敗しました
Failed to open stream on socket.Reason:error-info.	Socketでストリームを開くことができませんでした。理由はerror-infoです。
PAM initialization result:result-info.	PAM初期化の結果はresult-infoです
PAM:Failed to set attribute.Result:result-info.	PAMプロパティの設定がresult-infoで失敗しました
PAM:Sent a start-accounting request.Result:result-info.	PAMに対する課金開始要求が開始され、result-infoが返されます。
PAM:Sent a stop-accounting request.Result:result-info.	PAMへの終了課金要求は、result-infoとして返されます。
PAM:Resources released.	PAM関連リソースの解放
command	FTPクライアントがサーバに要求を送信するコマンド

4.2.14 ftp client source

Syntax

ftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo ftp client source

デフォルト

デバイスが FTP メッセージを送信するソース IP アドレスとして、ルートアウトインタフェースのプライマリ IP アドレスを使用するようにソースアドレスが設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*:FTP 転送に使用する送信元インタフェースを、インタフェースタイプとインタフェース番号を含めて設定します。このインタフェースに設定されているプライマリ IP アドレスが、送信メッセージの送信元アドレスです。プライマリ IP アドレスが設定され、状態が up のインタフェースを送信元インタフェースとして使用します。それ以外の場合、ファイル転送は失敗します。

ip *source-ip-address*:現在の FTP クライアントがメッセージを送信するために使用する送信元 IP アドレスを設定します。このアドレスは、デバイスですでに設定されている IP アドレスである必要があります。また、アドレスが設定されているインタフェースの状態が up である必要があります。そうでない場合、ファイル転送は失敗します。

説明

ftp client source コマンドを使用して、IPv 4 グループネットワーク環境で FTP クライアントから送信される FTP メッセージの送信元アドレスを設定します。

undo ftp client source コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最新のコマンドが有効になります。

本コマンドで送信元アドレスを指定した後、 ftp コマンドで送信元アドレスを指定すると、 ftp コマンドで指定した送信元アドレスで通信が行われる。

このコマンドで指定された送信元アドレスはすべての FTP 転送に対して有効であり、ftp コマンドで指定された送信元アドレスは現在の FTP 転送に対してのみ有効です。

例

#FTP メッセージを送信するようにデバイスを設定する送信元 IP アドレスは 192.168.20.222 です。

<Sysname> system-view

[Sysname] ftp client source ip 192.168.20.222

関連コマンド

- **ftp**

4.2.15 get

Syntax

get *remotefile [localfile]*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile:ダウンロードする必要があるファイルの名前。

localfile:ファイルをローカルにダウンロードするときに使用するファイル名。このパラメータを使用しない場合、ソースファイル名がローカルファイル名として保存されます。

説明

get コマンドは、FTP サーバからファイルをダウンロードし、ダウンロードしたファイルをローカルに保存します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

ファイルを保存する場合:

- ユーザが ftp コマンドを実行したときに、現在の作業ディレクトリにファイルを保存する場合、localfile はファイルの名前にするか、a.cfg のように入力しないでください。
- ユーザが ftp コマンドを実行したときに、現在の作業ディレクトリ以外のディレクトリにファイルを保存する場合は、localfile を flash:/subdirectory/a.cfg のような絶対パスにする必要があります。それ以外の場合、コマンドは失敗します。

例

#a.txt ファイルをダウンロードし、ユーザが ftp コマンドを実行したときの現在の作業ディレクトリに b.txt ファイル名で保存します。

ftp>get a.txt b.txt

```
local:b.txt remote:a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

#a.txt ファイルをダウンロードし、ユーザが ftp コマンドを実行したときのカレントワーキングディレクトリのサブフォルダ test に b.txt ファイル名で保存します。

ftp>get a.txt flash:/test/b.txt

```
local:flash:/test/b.txt remote:a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

関連コマンド

- **put**

4.2.16 help

Syntax

help *[command-name]*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

command-name:コマンド名。

説明

help コマンドを使用して、すべての FTP クライアントでサポートされているコマンドの名前を表示します。

help command-name コマンドは、指定したコマンドのヘルプ情報を表示します。

FTP クライアントビューの下で、help コマンドは同等ですか。コマンドを選択します。

例

#すべての FTP クライアントでサポートされているコマンドの名前を表示します。

ftp>help

```
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

#dir コマンドのヘルプを表示する

ftp>help dir

```
dir             list contents of remote directory
```

関連コマンド

- **?**

4.2.17 lcd

Syntax

lcd [*directory* | **/**]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory:このデバイス上のディレクトリを示します。このパラメータを使用して、FTP クライアントのローカルの作業ディレクトリを指定したディレクトリに切り替えます。ストレージメディア名の前には、「/flash:/logfile」のように 「/」 を付ける必要があります。

*/:*このデバイスのルートディレクトリを表します。このパラメータは、FTP クライアントのローカルの作業ディレクトリをアプライアンスのルートディレクトリに切り替えるために使用します。

説明

lcd コマンドを使用して、FTP クライアントのローカルの作業ディレクトリを表示または切り替えます。

パラメータを指定せずに lcd コマンドを実行すると、FTP クライアントのローカルの作業ディレクトリが表示されます。

例

#FTP クライアントのローカルの現在の作業ディレクトリを表示します。

ftp>lcd

```
Local directory now /flash:
```

#FTP クライアントのローカルワーキングディレクトリを flash:/logfile に切り替えます。

ftp>lcd /flash:/logfile

```
Local directory now /flash:/logfile
```

4.2.18 ls

Syntax

ls [*remotefile* [*localfile*]]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile:表示する FTP サーバ上のディレクトリまたはファイル名。

localfile:クエリ情報を保存するローカルファイルの名前。

説明

ls コマンドを使用して、FTP サーバの作業ディレクトリにあるすべてのサブディレクトリとファイルの詳細を表示します。この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

ls remotefile コマンドを使用して、FTP サーバ上のディレクトリまたはファイルの詳細を表示します。

ls remotefile localfile コマンドは、FTP サーバ上のディレクトリまたはファイルの詳細を localfile という名前のローカルファイルに保存します。

FTP クライアントビューでは、**ls** コマンドは **dir** コマンドと同じです。

例

#現在の FTP サーバの作業ディレクトリにあるすべてのフォルダとファイルの情報を表示します。

ftp> ls

```
150 Connecting to port 50201
-rwxr-xr-x   1 0        0             1481 Jul  7 15:36 a.txt
drwxr-xr-x   2 0        0             8192 Jul  2 14:33 diagfile
drwxr-xr-x   3 0        0             8192 Jul  7 15:21 ftp
drwxr-xr-x   2 0        0             8192 Jul  5 09:15 logfile
drwxr-xr-x   2 0        0             8192 Jul  2 14:33 seclog
-rwxr-xr-x   1 0        0         40808448 Jul  2 14:33 system-a1801.bin
-rwxr-xr-x   1 0        0             3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x   1 0        0            54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x   1 0        0             1481 Jul  7 12:34 x.cfg
226 9 matches total
```

#ファイル a.txt のクエリ結果を s.txt ファイルに保存します。

ftp>ls a.txt s.txt

```
output to local-file:s.txt?[Y/N] y
150 Connecting to port 50203
226-Glob:a.txt
```

s.txt ファイルの内容を確認します。

ftp>bye

```
221-Goodbye.You uploaded 0 and downloaded 2 kbytes.
221 Logout.
```

<Sysname> more s.txt

```
-rwxr-xr-x   1 0        0             1481 Jul  7 12:34 a.txt
```

関連コマンド

- **dir**

4.2.19 mkdir

Syntax

mkdir *directory*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory:作成するディレクトリの名前。

説明

mkdir コマンドを使用して、FTP サーバ上の現在の作業ディレクトリにサブディレクトリを作成します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

この操作を実行するには、ユーザに作成権限が必要です。

例

#FTP サーバの現在の作業ディレクトリにサブディレクトリ newdir を作成します。

ftp>mkdir newdir

```
257 "newdir":The directory was successfully created
```

4.2.20 newer

Syntax

newer *remotefile* [*localfile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile:ターゲットファイル名。

localfile:更新が必要なローカルファイルの名前。

説明

ローカルファイルを更新するには、**newer** コマンドを使用します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

ローカルファイルが存在しない場合、ターゲットファイルはローカルファイルより新しいとみなされます。つまり、ローカルファイルを更新する必要があります。

ターゲットファイルがローカルファイルより新しい場合、ローカルファイルは更新されません。

例

#FTP サーバのファイル a.txt ローカルより新しい､ローカルファイルを更新して下さい。

ftp>newer a.txt

```
local:a.txt remote:a.txt
150 Connecting to port 63513
226 File successfully transferred
1573 bytes received in 0.0293 seconds (52.3 kbyte/s)
```

4.2.21 open

Syntax

open *server-address* [*service-port*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

server-address:FTP サーバの IP アドレスまたはホスト名。

service-port:リモートデバイスが FTP サービスを提供する TCP ポート番号。範囲は 0~65535 で、デフォルト値は 21 です。

説明

open コマンドは FTP クライアントビューの下で FTP サーバにログインするのに使用されます。

ログインすると、ログインユーザ名とパスワードの入力を求めるプロンプトが表示されます。ユーザ名とパスワードが正しい場合、ログインは成功します。それ以外の場合、ログインは失敗します。

FTP サーバにログインしている場合は、**open** コマンドを使用して他の FTP サーバに直接接続することはできず、FTP サーバへの接続を中断してから再接続する必要があります。

例

#FTP クライアントビューで、FTP サーバにログインします(IP アドレス 192.168.40.7)。

<Sysname> ftp

ftp>open 192.168.40.7

```
Press CTRL+C to abort.
Connected to 192.168.40.7 (192.168.40.7).
220 FTP service ready.
User (192.168.40.7:(none)):root
331 Password required for root.
Password:
230 User logged in.
```

ftp>

4.2.22 passive

Syntax

passive

デフォルト

データ伝送方式はパッシブ方式である。

View

FTP client view

定義済みユーザロール

network-admin

説明

passive コマンドは、FTP データ転送のアクティブ/パッシブモードを切り替えるために使用します。

データ転送方式はアクティブ方式とパッシブ方式に分けられる。

- アクティブ方式とは、データ接続時に FTP サーバから接続要求をアクティブに行う方式である。
- パッシブ方式とは、データ接続が確立されたときに、FTP クライアントがアクティブに接続要求を開始することです。

このコマンドを繰り返して、FTP データ転送モードをアクティブまたはパッシブに設定します。

このコマンドは、プライベートユーザとパブリックユーザ間の FTP セッションを制限するために、主にファイアウォール機能とともに使用されます。

例

#データ転送のアクティブ/パッシブモードを切り替えます。

ftp>passive

```
Passive mode on.
```

ftp>passive

```
Passive mode off.
```

4.2.23 put

Syntax

put *localfile [remotefile]*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

localfile:アップロードするローカルファイルの名前。

remotefile:ファイルのアップロードが完了した後、FTP サーバに保存するときに使用するファイル名。ユーザが FTP サーバ上のファイル名を指定しない場合、デフォルトでは、このファイル名はローカルファイル名と同じになります。

説明

put コマンドを使用して、FTP クライアントのローカルファイルを FTP サーバにアップロードします。この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

ファイルを保存する場合:

- ユーザが ftp コマンドを実行したときにカレントワーキングディレクトリにあるファイルをアップロードする場合、localfile は a.cfg のようなファイル名になります。
- ユーザが ftp コマンドを実行したときに、カレントワーキングディレクトリ以外のファイルをアップロードする場合は、localfile を flash:/subdirectory/a.cfg のような絶対パスにする必要があります。それ以外の場合は、コマンドは失敗します。

例

#ユーザが ftp コマンドを実行したときのカレントワーキングディレクトリにある a.txt ファイルをアップロードし、b.txt ファイル名で保存します。

ftp>put a.txt b.txt

```
local:a.txt remote:b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

#ユーザが ftp コマンドを実行したときのカレントワーキングディレクトリのサブフォルダ test にある a.txt ファイルをアップロードし、b.txt ファイル名で保存します。

ftp>put flash:/test/a.txt b.txt

```
local:flash:/test/a.txt remote:b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

関連コマンド

- **get**

4.2.24 pwd

Syntax

pwd

View

FTP client view

定義済みユーザロール

network-admin

説明

pwd コマンドを使用して、現在のユーザがアクセスしている FTP サーバ上のディレクトリを表示します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

例

#現在のユーザがアクセスしている FTP サーバ上のディレクトリを表示します。

ftp>cd subdir

```
250 OK.Current directory is /subdir
```

ftp>pwd

```
257 "/subdir" is your current location
```

4.2.25 quit

Syntax

quit

View

FTP client view

定義済みユーザロール

network-admin

説明

quit コマンドを使用して、FTP サーバから切断し、User view に戻します。

例

#FTP サーバへの接続を終了し、User view に戻ります。

ftp>quit

```
221-Goodbye.You uploaded 0 and downloaded 0 kbytes.
221 Logout.
```

<Sysname>

関連コマンド

- **bye**

4.2.26 rhelp

Syntax

rhelp *[protocol-command]*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

protocol-command:FTP プロトコルコマンドワード。

説明

rhelp コマンドは、FTP サーバでサポートされている FTP 関連プロトコルのコマンドワードを表示するために使用します。

rhelp protocol-command コマンドを使用して、FTP サーバでサポートされている FTP 関連プロトコルのコマンドワードに関するヘルプ情報を表示します。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

例

#FTP サーバでサポートされている FTP 関連プロトコルのコマンドワードを表示します。

ftp>rhelp

```
214-The following FTP commands are recognized
 USER PASS NOOP QUIT SYST TYPE
 HELP CWD  XCWD PWD  CDUP XCUP
 XPWD LIST NLST MLSD PORT EPRT
 PASV EPSV REST RETR STOR APPE
 DELE MKD  XMKD RMD  XRMD ABOR
 SIZE RNFR RNTO
214 UNIX Type: L8
```

表 4-4 rhelp コマンドの表示情報の説明

フィールド	説明
214-The following FTP commands are recognized	使用可能なFTPコマンドワードのリストを次に示します。
USER	ユーザ名
PASS	ユーザパスワード
NOOP	空のアクションは、サーバが無効なコマンドを受信したときに何もしないことを示します。
QUIT	終了
SYST	システムパラメータの表示
TYPE	要求タイプ
HELP	助け
CWD	現在の作業ディレクトリを変更
XCWD	CWDを意味する拡張コマンド
PWD	印刷作業パス
CDUP	親ディレクトリへのディレクトリの変更
XCUP	拡張コマンド、CDUPと同じ意味
XPWD	拡張コマンド、PWDと同じ意味
LIST	ファイルを一覧表示
NLST	ファイルの簡単な説明を一覧表示

フィールド	説明
MLSD	ファイルの内容を一覧表示
PORT	アクティブモード(IPv4)
EPRT	アクティブモード(IPv6)
PASV	パッシブモード(IPv4)
EPSV	パッシブモード(IPv6)
REST	再起動
RETR	ファイルをダウンロード
STOR	ファイルをアップロード
APPE	追加アップロード
DELE	ファイルの削除
MKD	フォルダの作成
XMKD	拡張コマンド、MKDと同じ意味
RMD	フォルダの削除
XRMD	拡張コマンド、RMDと同じ意味
ABOR	割込み伝送
SIZE	ファイルの転送サイズの取得
RNFR	名前を変更するファイルの元の名前
RNTO	名前の変更が必要なファイルの新しい名前

4.2.27 rmdir

Syntax

rmdir *directory*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory:FTP サーバ上のディレクトリ名。

説明

rmdir コマンドを使用して、FTP サーバ上のディレクトリを完全に削除します。

注意

有用なディレクトリを誤って削除しないように、このコマンドを実行する前に、指定したディレクトリが使用されなくなったことを確認してください。

この操作は、FTP サーバへのログインに成功した場合にのみ実行できます。

この操作を実行するには、ユーザに削除権限が必要です。

削除するディレクトリは空である必要があります(ディレクトリを削除する前に、そのディレクトリにあるすべてのファイルとサブディレクトリを削除する必要があります。ファイルの削除については、**delete** コマンドを参照してください。)。

rmdir コマンドが正常に実行されても、FTP サーバのごみ箱にある元のファイルは削除されません。

例

#空のディレクトリ subdir1 を削除します。

ftp>rmdir subdir1

```
250 The directory was successfully removed
```

関連コマンド

- **delete**

4.2.28 user

Syntax

user *username* [*password*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

username:ログインユーザ名。

password:ログインパスワード。

説明

user コマンドを使用して、既存の FTP 接続で FTP 認証を再起動します。認証が成功すると、現在の FTP サーバにアクセスできます。

このコマンドは通常、次の場合に使用します。

- ユーザが FTP サーバにログインできませんでした。FTP 接続がタイムアウトになる前に、このコマンドを使用して現在アクセスされている FTP サーバに再ログインしてください。
- ユーザは FTP サーバに正常にログインしました。このコマンドを使用して、現在アクセスしている FTP サーバに別のユーザとして再ログインします。

このコマンドを使用する前に、FTP サーバで適切なユーザ名とパスワードを設定する必要があります。設定しないと、ログインが失敗し、FTP 接続が閉じられます。

例

#ユーザが FTP サーバにログインしました。現在の FTP サーバに新しい ID (ユーザ名 ftp、パスワード 123456)で再ログインします。

方法 1:

ftp>user ftp 123456

```
331 Password required for ftp.
230 User logged in.
```

方法 2:

ftp>user ftp

```
331 Password required for ftp.
Password:
230 User logged in.
```

4.2.29 verbose

Syntax

verbose

デフォルト

FTP 操作の詳細を表示できます。

View

FTP client view

定義済みユーザロール

network-admin

説明

verbose コマンドは、FTP 操作中の詳細の表示を許可または禁止するために使用します。

この設定は、現在のセッションでのみ有効です。ユーザが再度ログインすると、このコマンドはデフォルトに戻ります。

例

#FTP 操作中の詳細が表示されない場合は、get 操作を行います。

ftp>verbose

```
Verbose mode off.
```

ftp>get a.cfg 1.cfg

#FTP 操作中の詳細が表示されたら、get 操作を実行できます。

ftp>verbose

```
Verbose mode on.
```

ftp>get a.cfg 2.cfg

```
227 Entering Passive Mode (192,168,1,58,68, 14)
150-Accepted data connection
150 The computer is your friend.Trust the computer
226 File successfully transferred
3796 bytes received in 0.00762 seconds (486.5 kbyte/s)
```

目次

このセクションのページは **2-x-x** です。

5 章 TFTP 5-1
5.1 TFTP 設定コマンド 5-1
5.1.1 tftp 5-1
5.1.2 tftp client source 5-4
5.1.3 tftp-server acl 5-6

5章 TFTP

5.1 TFTP設定コマンド

5.1.1 tftp

Syntax

tftp *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] * [**-d**]

View

User view

定義済みユーザロール

network-admin

パラメータ

tftp-server:TFTP サーバの IP アドレスまたはホスト名。ここで、ホスト名は 1~253 文字の文字列で、大文字と小文字は区別されません。文字列には、英字、数字、「-」、「_」、または 「.」 のみを使用できます。

get:ファイルのダウンロードを実行します。この操作を行うと、デバイスはファイルをストレージメディアに直接保存します。ダウンロードする前に同じ名前のファイルがすでにストレージメディアに存在する場合は、ダウンロードする前にストレージメディアの既存のファイルを削除します。ダウンロードに失敗すると、既存のファイルが削除され、復元できなくなるため、安全ではありません。

put:ファイルのアップロードを実行します。

sget:ファイルの安全なダウンロードを実行します。この操作を実行すると、デバイスはファイルをメモリに保存し、保存に成功すると、ストレージメディアにコピーしてメモリ内のファイルを削除します。get 方式よりも安全です。

source-filename:ソースファイル名。1~255 文字の文字列で、大文字と小文字は区別されません。

destination-filename:ターゲットファイル名。1~255 文字の文字列で、大文字と小文字は区別されません。このパラメータを指定しない場合は、ソースファイル名がターゲットファイル名として使用されます。

dscp *dscp-value*:デバイスが送信する TFTP メッセージに含まれる DSCP の優先度を 0~63 の範囲で指定します。デフォルトは 0 です。

source:送信された TFTP メッセージの送信元 IP アドレス。このパラメータが指定されていない場合、送信された TFTP メッセージの送信元 IP アドレスとして、ルーティングされたインタフェースのプライマリ IP アドレスが使用されます。

interface *interface-type interface-number*:デバイスから送信される TFTP メッセージの送信元 IP アドレスとして、このインタフェースに設定されているプライマリ IP アドレスを持つ送信元インタフェースのタイプと数を示します。プライマリ IP アドレスが設定され、状態が up のインタフェースを送信元インタフェースとして使用します。それ以外の場合、ファイル転送は失敗します。

ip *source-ip-address*:デバイスから送信される TFTP メッセージの送信元 IP アドレスになる送信元 IP アドレス。このアドレスは、デバイスですでに設定されている IP アドレスである必要があります。また、アドレスが設定されているインタフェースの状態が up である必要があります。そうでない場合、ファイル転送は失敗します。

-d:TFTP クライアントデバッグ情報スイッチをオンにします。デフォルトはオフです。

説明

tftp コマンドを使用して、IPv 4 グループネットワーク環境で次の操作を行います。

- ファイルのダウンロード:TFTP サーバからローカルにソースファイルをダウンロードします。
- ファイルのアップロード:ローカルのソースファイルを TFTP サーバにアップロードします。

tftp client source コマンドで送信元アドレスを指定したあと、tftp コマンドで送信元アドレスを指定すると、**tftp** コマンドで指定した送信元アドレスで通信が行われます。

tftp client source コマンドで指定された送信元アドレスはすべての TFTP 転送に有効であり、**tftp** コマンドで指定された送信元アドレスは現在の TFTP 転送にのみ有効です。

例

#TFTP サーバ上の new.bin ファイルをローカルストレージデバイスにダウンロードします。TFTP サーバの IP アドレスは 192.168.1.1 で、ローカルにダウンロードしてファイル名 new.bin で保存する。

<AC> tftp 192.168.1.1 get new.bin

```
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   183  100   183    0     0    640      0 --:--:-- --:--:-- --:--:--  1830
100   183  100   183    0     0    629      0 --:--:-- --:--:-- --:--:--   629
```

表 5-1 tftp コマンドの表示情報の説明

フィールド	説明
%	ファイル転送の進捗率
Total	転送するファイルのサイズをバイト単位で指定します。
%	ダウンロード時に受信したファイルの合計サイズに対する割合

フィールド	説明
Received	ダウンロード時に受信したファイルのバイト単位のサイズ
%	アップロード時に送信されたファイルの合計サイズに対する割合
Xferd	アップロード時に送信されたファイルのバイト単位のサイズ
Average Dload	バイト/秒の平均ダウンロード速度
Speed Upload	バイト/秒の平均アップロード速度
Time Total	ファイル転送にかかった時間と残り時間の合計を秒単位で表したもの
Time Spent	ファイル転送に秒単位で時間がかかりました
Time Left	ファイル転送の完了に要する秒数
Current Speed	バイト/秒単位のファイル転送時の現在の速度

表 5-2 tftp クライアントのデバッグ情報の説明

フィールド	説明
TFTP_STATE_START	TFTPサービスの開始
File not found	ターゲットファイルが見つかりません
DO phase is complete	操作が完了しました
Connection time-out	接続タイムアウト
TFTP response timeout	応答タイムアウト
Data size exceeds single call write limit	データ長がライトバック制限を超えています
INTERNAL CONFUSION	内部転送データの混乱
Internal error clearing splay node	ノード上のデータの消去中に内部エラーが発生しました
Could not open socket pair.	ソケットペアを開くことができません
Could not fork	プロセスを作成できません
Received too short packet	受信データが短すぎます
Internal error Unexpected packet	内部エラー、予期しないパケット
STATE:INIT =>	状態:初期化
Trying ip-address	接続を試行中ip-address
STATE:CONNECT =>	状態:接続
Connected to ip-address () port port-id	ip-addressに接続します。ポート番号はport-idです。
bind () failed;	バインドに失敗しました
STATE:WAITCONNECT =>	ステータス:接続の待機
STATE:SENDPROTOCONNECT =>	ステータス:プロトコル接続の開始
Added connection	接続の追加
set timeouts for state 0:	ステータス0のタイムアウト時間の設定
STATE:DO=>	ステータス:操作の開始
got option=(parameter) value=(value)	パケット包含オプションparameterを受信しました。値はvalueです。

フィールド	説明
requested (size)	要求パケットの長さはsizeバイトです
blksize parsed from OACK (size)	OACK応答パケットの長さはsizeバイトです。
Server requested blksize larger than allocated	サービス要求データ長の超過
Connected for receive	ファイル接続の受信
Connected for transmit	ファイル接続の転送
TFTP_STATE_RX	TFTPサービスステータスがデータを受信しています
TFTP_STATE_TX	TFTPサービスの状態は、データを転送しています
Internal state machine error	内部状態エラー
Receive last DATA packet block %d again	最後のパケットをもう一度受信します
Received unexpected DATA packet block %d、expecting block %d	不正なパケット(長さ:%d)を受信しました。正しいデータ長は%d、バイトです。
Timeout waiting for block %d ACK.Retries =	ACK要求タイムアウト、再要求
Received ACK for block %d、expecting	正しいACK応答を受信しました
tftp_tx:giving up waiting for block %d ack	TFTP転送:ACK応答の待機を破棄します。
tftp_rx:internal error	TFTP受信データ:内部エラー
tftp_tx:internal error, event:event-info	TFTP転送データ:内部エラー、イベント:event-info
STATE:DOING =>	状態:操作
STATE:DO_DONE =>	ステータス:操作完了
multi_done	マルチプロセッシング完了
TFTP finished	TFTP完了
Closing connection 0	接続0を閉じる
The cache now contains 0 members	現在のバッファが空です
TFTP:Illegal operation	不正操作
Expire cleared	TFTPサービス終了

関連コマンド

- **tftp client source**

5.1.2 tftp client source

Syntax

tftp client source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo tftp client source

デフォルト

TFTP メッセージを送信するデバイスの送信元 IP アドレスとして、ルーティングアウトインターフェイスのプライマリ IP アドレスを使用する送信元アドレスは設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*:TFTP 転送に使用する送信元インタフェースを設定します。インタフェースタイプとインタフェース番号が含まれ、このインタフェースに設定されたプライマリ IP アドレスが送信元アドレスになります。プライマリ IP アドレスが設定され、状態が up のインタフェースを送信元インタフェースとして使用します。それ以外の場合、ファイル転送は失敗します。

ip *source-ip-address*:現在の TFTP クライアントがメッセージを送信するために使用する送信元 IP アドレスを設定します。このアドレスは、デバイスですでに設定されている IP アドレスである必要があります。また、アドレスが設定されているインタフェースの状態が up である必要があります。そうでない場合、ファイル転送は失敗します。

説明

tftp client source コマンドを使用して、IPv 4 グループネットワーク環境で TFTP クライアントが送信する TFTP メッセージの送信元アドレスを設定します。

undo tftp client source コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最新のコマンドが有効になります。

本コマンドで送信元アドレスを指定した後、 **tftp** コマンドで送信元アドレスを指定すると、 **tftp** コマンドで指定した送信元アドレスで通信が行われる。

このコマンドで指定された送信元アドレスはすべての TFTP 転送に対して有効であり、**tftp** コマンドで指定された送信元アドレスは現在の TFTP 転送に対してのみ有効です。

例

#TFTP メッセージを送信するようにデバイスを設定する送信元 IP アドレスは 192.168.20.222 です。

<AC> system-view

[AC] tftp client source ip 192.168.20.222

関連コマンド

- **tftp**

5.1.3 tftp-server acl

Syntax

tftp-server *acl acl-number*

undo tftp-server acl

デフォルト

デバイスがアクセスできる TFTP サーバを制限するために ACL は使用されません。

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number:基本アクセス制御リストの番号。範囲は 2000~2999 です。

説明

IPv 4 グループネットワーク環境で ACL を使用して、デバイスがアクセスできる TFTP サーバを制限するには、**tftp-server acl** コマンドを使用します。

undo tftp-server acl コマンドを使用して、デフォルトの状態を復元します。

ユーザは、ACL で設定されたルールを使用して、ネットワーク上の特定の TFTP サーバへのデバイスアクセスを許可または禁止できます。

例

#IP アドレスが 1.1.1.1 の TFTP サーバにのみデバイスがアクセスできるようにします。

<AC> system-view

[AC] acl basic 2000

[AC-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0

[AC-acl-ipv4-basic-2000] quit

[AC] tftp-server acl 2000

目次

このセクションのページは **2-x-x** です。

6 章 ファイルシステム管理 6-1
6.1 ファイルシステム管理コマンド 6-1
6.1.1 cd 6-1
6.1.2 copy 6-2
6.1.3 delete 6-5
6.1.4 dir 6-7
6.1.5 file prompt 6-9
6.1.6 fixdisk 6-9
6.1.7 format 6-10
6.1.8 gunzip 6-11
6.1.9 gzip 6-12
6.1.10 mkdir 6-13
6.1.11 more 6-14
6.1.12 mount 6-15
6.1.13 move 6-16
6.1.14 pwd 6-16
6.1.15 rename 6-17
6.1.16 reset recycle-bin 6-18
6.1.17 rmdir 6-19
6.1.18 tar create 6-20
6.1.19 tar extract 6-21
6.1.20 tar list 6-22
6.1.21 umount 6-23
6.1.22 undelete 6-24

6章 ファイルシステム管理

6.1 ファイルシステム管理コマンド

注意

- 重要なファイル/フォルダを誤って削除しないように、ファイル/フォルダの機能を十分に理解してから、各種のファイル/フォルダ操作を実行してください。
- ファイル/フォルダは非表示、非表示に分類されます。非表示のファイル/フォルダは、対応する機能に影響を与えるため、変更または削除しないでください。
- ファイル/フォルダに名前を付ける場合、頭文字に 「.」 は使用できません。それ以外の場合は、名前の頭文字が 「.」 のファイル/フォルダが非表示として認識されます。

copy、delete、fixdisk、format、gunzip、gzip、mkdir、move、rename、rmdir、undelete コマンドなど、ストレージメディアへの書き込みが必要な場合は、ストレージメディアが書き込み保護されていないことを確認します。ストレージメディアが書き込み保護されている場合、これらのコマンドは失敗します。他のコマンドラインの実行は、書き込み保護スイッチの影響を受けません。

ユーザがストレージメディアまたはファイルシステムに対して fixdisk、format、fdisk のいずれかの操作を実行すると、他のユーザはストレージメディアまたはファイルシステムにアクセスできなくなります。これらの操作が完了するまで待ってから、次の方法でストレージメディアまたはファイルシステムにアクセスします。

- コマンドライン引数を使用して、絶対パスを直接指定します。たとえば、dir flash:/ コマンドを使用して Flash のファイルを表示します。
- 相対パスを使用してアクセスする前に、cd コマンドでストレージメディアまたはファイルシステムディレクトリに移動します。たとえば、cd flash:/を使用して Flash にアクセスし、dir コマンドを使用して Flash のファイルを表示します。

このコマンドマニュアルに記載されているファイルシステム名、ディレクトリ名、ファイル名のパラメータ入力規則は、ファイルシステム命名規則に準拠している必要があります。詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*10 章 ファイルシステム管理*”を参照してください。

6.1.1 cd

Syntax

cd { *directory* | **..** }

View

User view

定義済みユーザロール

network-admin

パラメータ

directory:ターゲットワークパスを指定します。

..:前のレベルのディレクトリを返します。現在の作業パスがルートの場合は、cd ..の実行後にエラーが表示されます。このパラメータは、コマンドラインオンラインヘルプをサポートしていません。

説明

cd コマンドは、作業パスを変更します。

例

#デバイスにログインしたら、ルートディレクトリから test フォルダに移動します。

<Sysname> cd test

#前のレベルのディレクトリを返します。

<Sysname> cd ..

6.1.2 copy

Syntax

copy *source-file* { *dest-file* | *dest-directory* } [**source interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file:ソースファイル名またはリモートソースファイルの URL。URL 形式の場合は、リモートファイルサーバからファイルをコピーします。リモートソースの URL が大文字と小文字をサポートするかどうかは、リモートサーバ側の仕様に従います。

dest-file:ターゲットファイル名またはリモートターゲットファイルの URL。URL 形式の場合は、リモートのターゲットファイルにファイルをコピーします。リモートターゲットファイルの URL が大文字と小文字をサポートするかどうかは、リモートサーバ側の仕様に従います。

dest-directory:ターゲットフォルダまたはリモートディレクトリの URL。URL 形式の場合は、リモートの宛先フォルダにファイルをコピーします。リモートディレクトリ URL が大文字と小文字をサポートするかどうかは、リモートサーバ側の仕様に従います。フォルダを dest-directory として使用すると、ファイルはソースファイル名をファイル名として使用してフォルダにコピーされます。

source interface *interface-type interface-number*:リモートサーバへの接続に使用するソース・インタフェースを指定します。送信元インタフェースを指定すると、デバイスは送信元インタフェースのプライマリ IP を、デバイスが生成した接続メッセージの送信元 IP として使用します。このパラメータを指定しない場合は、発信元インタフェースとしてルーティングされた発信インタフェースが使用されます。

説明

copy コマンドを使用してファイルをコピーします。

source-file および dest-file を指定する場合:

- source-file と dest-file の両方がローカル・パスである場合、ローカル・ファイル間のコピーが可能です。
- source-file がリモートサーバ上のパス(URL 形式)で、dest-file にローカル・パスが指定されている場合は、リモートサーバ上のファイルをローカルにコピーできます。
- ローカル・ファイルをリモートサーバにコピーできるのは、source-file がローカル・パスで、dest-file がリモートサーバ上のパス(URL 形式)の場合です。

リモート・コピーの場合は、FTP、TFTP、HTTP の各プロトコルがサポートされており、各プロトコルの URL 形式は表 6-1 のとおりです。

表 6-1 FTP、TFTP、および HTTP プロトコルの URL 形式

プロトコル・タイプ	URL フォーマット	説明
FTP	ftp://FTPユーザ名[:パスワード]@サーバアドレス[:ポート番号]/ファイルパス	ユーザ名とパスワードは、サーバの構成と一致している必要があります。たとえば、ftp :// a:1@1.1.1.1/startup.cfgは、1.1.1.1というアドレスのFTPサーバ認証ディレクトリにあるstartup.cfgファイルを表し、ユーザ名はa、パスワードは1です。 サーバがユーザ名のみを認証する場合は、パスワードを入力する必要はありません。
TFTP	tftp ://サーバアドレス[:ポート番号]/ファイルパス	t ftp://1.1.1.1/startup.cfgは、アドレス1.1.1.1のTFTPサーバの作業ディレクトリにあるstartup.cfgファイルを表します。

プロトコル・タイプ	URL フォーマット	説明
HTTP	http://HTTPユーザ名[:パスワード]@サーバアドレス[:ポート番号]/ファイルパス	ユーザ名とパスワードは、サーバの構成と一致している必要があります。たとえば、http :// a:1@1.1.1.1/startup.cfgは、アドレス1.1.1.1のHTTP Server認証ディレクトリにあるstartup.cfgファイルを表し、ログインユーザ名はa、パスワードは1です。 サーバがユーザ名のみを認証する場合は、パスワードを入力する必要はありません。 サーバが認証を必要としない場合は、URLにユーザ名とパスワードを入力する必要はありません。たとえばhttp://1.1.1.1/startup.cfgの場合は、アドレス1.1.1.1のHTTPサーバの作業ディレクトリにあるstartup.cfgファイルを表す.

サーバアドレスがIPv 6アドレスの場合、IPv 6アドレスとポート番号を区別するために、IPv 6 アドレスを中括弧「[]」で囲む必要があります。例:ftp://test:test@ [2001::1]:21/test.cfg ここで、2001::1 は FTP サーバの IPv 6 アドレス、21 は FTP プロトコルのポート番号です。

例

#ファイル test.cfg を現在のフォルダにコピーし、testbackup.cfg という名前を付けます。

<Sysname> copy test.cfg testbackup.cfg

```
Copy flash:/test.cfg to flash:/testbackup.cfg?[Y/N]:y
Copying file flash:/test.cfg to flash:/testbackup.cfg ... Done.
```

#Flash 上のフォルダ test の下のファイル 1.cfg を、指定された USB ドライブのフォルダ testbackup にコピーし、1 backup.cfg という名前を付けます。

<Sysname> copy flash:/test/1.cfg usba0:/testbackup/1backup.cfg

```
Copy flash:/test/1.cfg to usba0:/testbackup/1backup.cfg?[Y/N]:y
Copying file flash:/test/1.cfg to usba0:/testbackup/1 backup.cfg ... Done.
```

#デバイスにログインしたら、指定したスロットのルートディレクトリにプロファイルをコピーします。

<Sysname> copy test.cfg slot2#flash:/

```
Copy flash:/test.cfg to slot2#flash:/test.cfg?[Y/N]:y
Copying file flash:/test.cfg to slot2#flash:/test.cfg ... Done.
```

#FTP サーバ 1.1.1.1 上のファイル test.cfg を testbackup.cfg という名前でローカルにコピーします。FTP サーバのログインユーザ名は user、パスワードは private です。

<Sysname> copy ftp :// user:private@1.1.1.1/test.cfg testbackup.cfg

```
Copy ftp :// user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg?[Y/N]:y
Copying file ftp :// user:private@1.1.1.1/test.cfg to
flash:/testbackup.cfg ...Done.
```

#ファイル test.cfg を testbackup.cfg という名前で FTP サーバ 1.1.1.1 にコピーします。FTP サーバのログインユーザ名は user、パスワードは private です。

<Sysname> copy test.cfg ftp :// user:private@1.1.1.1/testbackup.cfg

```
Copy flash:/test.cfg to ftp :// user:private@1.1.1.1/testbackup.cfg?[Y/N]:y
Copying file flash:/test.cfg to ftp ://
user:private@1.1.1.1/testbackup.cfg ...Done.
```

#TFTP サーバ 1.1.1.1 のファイル test.cfg をローカルにコピーし、testbackup.cfg という名前を付けます。

<Sysname> copy t ftp://1.1.1.1/test.cfg testbackup.cfg

```
Copy t ftp://1.1.1.1/test.cfg to flash:/testbackup.cfg?[Y/N]:y
Copying file t ftp://1.1.1.1/test.cfg to flash:/testbackup.cfg ...Done.
```

#ファイル test.cfg を TFTP サーバ 1.1.1.1 にコピーし、testbackup.cfg という名前を付けます。

<Sysname> copy test.cfg t ftp://1.1.1.1/testbackup.cfg

```
Copy flash:/test.cfg to t ftp://1.1.1.1/testbackup.cfg?[Y/N]:y
Copying file flash:/test.cfg to t ftp://1.1.1.1/testbackup.cfg ...Done.
```

#HTTP Server 1.1.1.1 のファイル test.cfg をローカルにコピーし、testbackup.cfg という名前を付けます。HTTP Server のログインユーザ名は user、パスワードは private です。

<Sysname> copy http :// user:private@1.1.1.1/test.cfg testbackup.cfg

```
Copy http :// user:private@1.1.1.1/test.cfg to flash:/testbackup.cfg?[Y/N]:y
Copying file http :// user:private@1.1.1.1/test.cfg to
flash:/testbackup.cfg ...Done.
```

#ファイル test.cfg を testbackup.cfg という名前で HTTP Server 1.1.1.1 にコピーします。HTTP Server のログイン名は user、パスワードは private です。

<Sysname> copy test.cfg http :// user:private@1.1.1.1/testbackup.cfg

```
Copy flash:/test.cfg to http :// user:private@1.1.1.1/testbackup.cfg?[Y/N]:y
Copying file flash:/test.cfg to http ://
user:private@1.1.1.1/testbackup.cfg ...Done.
```

6.1.3 delete

Syntax

delete [**/unreserved**] *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

/unreserved:ファイルを完全に削除します。このパラメータを指定しない場合、削除されたファイルはごみ箱に移動されます。

file:削除するファイルの名前。file パラメータでは、ワイルドカード文字 「*」 を使用した照合がサポートされています。たとえば、delete *.txt は、現在のディレクトリにある txt 拡張子を持つすべてのファイルを削除します。

説明

delete コマンドを使用してファイルを削除します。

 注意

- **delete /unreserved file** コマンドは、デバイスから完全に削除されるファイルを完全に削除するために使用します。削除されたファイルはもう存在しないため、リカバリできません。

---

delete file コマンドは、ファイルを一時的に削除します。削除されたファイルはごみ箱に保存され、**undelete** コマンドを使用して復元できます。

ファイルシステムの領域が不足している場合は、**delete /unreserved file** コマンドを実行すると、対応するファイルが完全に削除されます。

ごみ箱内のファイルに対して delete コマンドを実行しないでください。これはごみ箱の機能に影響します。ごみ箱からファイルを削除するには、reset recycle-bin コマンドを使用します。

同じディレクトリ内で同じ名前のファイルを 2 つ削除した場合、最後に削除したファイルだけがごみ箱に残ります。異なるディレクトリで同じ名前のファイルを削除した場合、削除したファイルはごみ箱に残ります。

例

#現在のディレクトリにあるファイル 1.cfg を削除します。

<Sysname> delete 1.cfg

```
Delete flash:/1.cfg?[Y/N]:y
Deleting file flash:/1.cfg ... Done.
```

#現在のディレクトリにあるファイル 1.cfg を完全に削除します。

<Sysname> delete /unreserved 1.cfg

```
The file cannot be restored.Delete flash:/1.cfg?[Y/N]:y
Deleting the file permanently will take a long time.Please wait ...
Deleting file flash:/1.cfg ... Done.
```

関連コマンド

- **undelete**
- **reset recycle-bin**

6.1.4 dir

Syntax

dir [**/all**] [*file* | *directory* | **/all-filesystems**]

View

User view

定義済みユーザロール

network-admin

パラメータ

/all:非表示ファイル、非表示フォルダ、非表示ファイル、非表示フォルダなど、現在のフォルダの下にあるすべてのファイルとフォルダの情報を表示します。このパラメータを指定しない場合、非表示のファイルと非表示のフォルダのみが表示されます。

file:指定したファイルの情報を表示します。file 引数は、ワイルドカード文字 「*」 をサポートしています。たとえば、dir*.txt は、現在のフォルダの下にある txt 拡張子を持つすべてのファイルを表示します。

directory:指定したフォルダの情報を表示します。

/all-filesystems:デバイス上のすべてのファイルシステムのルートにあるファイルとフォルダの情報を表示します。

説明

dir コマンドは、現在のフォルダまたはファイル情報を表示します。

パラメータを指定しない場合、現在のフォルダの下にあるすべての表示可能なファイルとフォルダの情報を表示します。

ごみ箱のフォルダ名は「.trash」です。ごみ箱内のファイルを表示するには、dir /all .trash または cd .trash でごみ箱フォルダに移動し、dir コマンドを使用します。

ファイルやフォルダを同時に作成または削除するなど、複数のユーザが同時にファイル操作を実行すると、コマンドの表示結果が不正確になることがあります。

例

#現在のフォルダの下にあるすべてのファイルとフォルダ情報を表示します。

<Sysname> dir /all

Directory of flash:/

...

#デバイス上のすべてのファイルシステムのルートにあるファイルとフォルダの情報を表示します。

<Sysname> dir /all-filesystems

```
Directory of flash:/
...

Directory of usba0:/
...
```

表 6-2 dir コマンドによる情報説明の表示

フィールド	説明
Directory of	現在表示されているディレクトリ
0-rwh3144Jan 26 2020 13:45:28xx.xx	ファイルまたはフォルダの情報: • 0 は番号で、システムによって自動的に割り当てられます。 • -rwh は属性を表します。最初の文字が 「d」 の場合はフォルダ、 「-」 の場合はファイル;2 番目の文字は r で、このファイルまたはフォルダが読み取り可能であることを示します。3 番目の文字は w で、このファイルまたはフォルダが書き込み可能であることを示します。4 番目の文字が h の場合は、ファイルまたはフォルダが非表示であることを示し、 「-」 の場合は非表示であることを示します(非表示のファイルやフォルダは、対応する機能に影響を与えないように変更または削除しないでください。)。 • 3144 はファイルサイズで、単位は B です。「-」 と表示されている場合は、フォルダであることを示します。 • Jan 26 2020 13:45:28 は、最新の変更時刻を示します。 • xx.xx は名前です。

6.1.5 file prompt

Syntax

file prompt { **alert** | **quiet** }

undo file prompt

デフォルト

ユーザがファイルに対して危険な操作を行った場合、システムはユーザに対話的な確認を求める。

View

System view

定義済みユーザロール

network-admin

パラメータ

alert:ユーザがファイル/フォルダに対して危険な操作を行った場合、ユーザは対話形式で確認するよう求められます。

quiet:ユーザがファイル/フォルダに対してごみ箱を空にする以外の操作を行った場合、ユーザは確認を求められません。

説明

file prompt コマンドは、ファイル/フォルダに対するシステム操作のプロンプトを設定します。

undo file prompt コマンドを使用して、デフォルトの状態を復元します。

ファイル/フォルダ操作のヒントを quiet に設定すると、ごみ箱を空にする以外のファイル/フォルダ操作ではユーザの確認が不要になり、誤操作による回復不能なシステム障害が発生する可能性があります。

例

#セットアップユーザがファイルに対して危険な操作を行った場合、対話的な確認を要求する。

<Sysname> system-view

[Sysname] file prompt alert

6.1.6 fixdisk

Syntax

fixdisk *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem:ファイルシステムの名前。

説明

fixdisk コマンドを使用して、ファイルシステムの領域をリカバリします。

ファイルシステムの一部の領域は、例外操作などの理由で使用できない場合や、不要になったが解放されない場合があります。ユーザは、fixdisk コマンドを使用してファイルシステムの領域をリストアできます。

ユーザがファイルシステムに対して fixdisk 操作を実行しているときに、他のユーザがそのファイルシステムにアクセスしている場合は、fixdisk 操作が失敗したことを示すメッセージが表示されます。

例

#ファイルシステム Flash の領域をリストアします。

<Sysname> fixdisk flash:

```
Restoring flash:may take some time ...
Restoring flash :... Done.
```

6.1.7 format

Syntax

format *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem:ファイルシステムの名前。

説明

format コマンドは、ファイルシステムのフォーマットに使用されます。

注意

フォーマット操作を行うと、ファイルシステム内のすべてのファイルが失われ、リカバリできなくなります。特に、ファイルシステムに起動プロファイルがある場合、ファイルシステムをフォーマットすると起動プロファイルが失われることに注意してください。

プラグ可能なストレージメディアの場合、デバイスは VFAT タイプのファイルシステムのみをサポートしています。VFAT タイプのファイルシステムでない場合は、読み取りと書き込みのために VFAT タイプにフォーマットする必要があります。

ユーザがファイルシステムのフォーマット操作を実行するときに、他のユーザがファイルシステムにアクセスしている場合は、フォーマット操作が失敗したことを示すメッセージが表示されます。

フォーマットするファイルシステムにセキュリティ・ログ・ファイルが存在する場合は、フォーマットできません。必要に応じて、ファイルシステムからセキュリティログを削除してください。セキュリティログは、セキュリティログ管理者が操作する必要があります。セキュリティログ管理者の詳細には、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。

例

#書式設定 flash:。

<Sysname> format flash:

```
All data on flash:will be lost, continue?[Y/N]:y
Formatting flash :...Done.
```

#USB メモリの 3 番目のパーティションをフォーマットします。

<Sysname> format usba2:

```
All data on usba2:will be lost, continue?[Y/N]:y
Formatting usba 2 :...Done.
```

6.1.8 gunzip

Syntax

gunzip *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file:解凍する必要があるファイル名。 .gz が接尾辞になります。

説明

gunzip コマンドを使用してファイルを解凍します。

このコマンドは、現在指定されているファイルを解凍して置き換えます。

例

#system.bin.gz ファイルを解凍します。

- 解凍する前にファイルに関する情報を表示します。

<Sysname> dir system.*

```
Directory of flash:
1-rw-20 Jan 14 2020 10:18:53system.bin.gz


1048576 KB total (472840 KB free)
```

- 解凍操作を実行します。

<Sysname> gunzip system.bin.gz

```
Decompressing file flash:/system.bin.gz .....Done.
```

- 解凍後に実行結果を確認します。

<Sysname> dir system.*

```
Directory of flash:
1-rw-0 Jan 30 2020 11:42:25system.bin


1048576 KB total (472844 KB free)
```

6.1.9 gzip

Syntax

gzip *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file:圧縮する必要があるファイルの名前。

説明

gzip コマンドを使用してファイルを圧縮します。

このコマンドを実行すると、元のファイルは圧縮され、file.gz という名前が付けられ、削除されます。

例

#system.bin ファイルを圧縮します。

- 圧縮する前にファイルに関する情報を表示します。

<Sysname> dir system.*

```
Directory of flash:
1-rw-0 Jan 30 2020 11:42:24system.bin


1048576 KB total (472844 KB free)
```

- 圧縮操作を実行します。

<Sysname> gzip system.bin

```
Compressing file flash:/system.bin .....Done.
```

- 圧縮後に実行結果を確認します。

<Sysname> dir system.*

```
Directory of flash:
1-rw-20 Jan 14 2020 10:18:53system.bin.gz


1048576 KB total (472840 KB free)
```

6.1.10 mkdir

Syntax

mkdir *directory*

View

User view

定義済みユーザロール

network-admin

パラメータ

directory:フォルダ。

説明

mkdir コマンドを使用してフォルダを作成します。

指定したフォルダの下にあるファイルまたは別のフォルダと同じ名前のフォルダを作成すると、作成は失敗します。

このコマンドを使用してフォルダを作成する前に、指定したフォルダがすでに存在している必要があります。たとえば、フォルダ flash:/test/mytest を作成する場合、test フォルダはすでに存在している必要があります。存在していない場合、作成は失敗します。

例

#現在のパスに test フォルダを作成します。

<Sysname> mkdir test

```
Creating directory flash:/test ...Done.
```

#現在のパスにフォルダ test/subtest を作成します。

<Sysname> mkdir test/subtest

```
Creating directory flash:/test/subtest ...Done.
```

6.1.11 more

Syntax

more *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file:ファイル名。

説明

more コマンドは、テキストファイルの内容を表示します。

例

#ファイル test.txt の内容を表示します。

<Sysname> more test.txt

```
Have a nice day.
```

#ファイル testcfg.cfg の内容を表示します。

<Sysname> more testcfg.cfg

```
#
version 7.1.070、Release 1201
#
sysname Sysname
#
vlan 2
#
return
```

<Sysname>

6.1.12 mount

Syntax

mount *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem:ファイルシステムの名前。

説明

mount filesystem コマンドは、ファイルシステムをマウントするために使用します。

ストレージメディアをデバイスに接続すると、ファイルシステムが自動的にマウントされます。システムが自動的に認識されない場合は、マウント操作を手動で実行しないと、ファイルシステムの読み取りと書き込みを実行できません。

マウント操作中は、ファイルシステムの破損を防ぐために、次のようなストレージメディアの操作は禁止されています。

- ストレージメディアの抜き差しを禁止します。
- デバイスの再起動や電源オフを無効にします。

マウントされているストレージメディアファイルシステムが破損しないように、システムを取り外す前にアンマウント操作を実行してください。

例

#USB ファイルシステムをマウントします。

<Sysname> mount usba0:

関連コマンド

- **umount**

6.1.13 move

Syntax

move *source-file {dest-file |dest-directory }*

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file:ソースファイル名。

dest-file:ターゲットファイル名。

dest-directory:宛先フォルダ。

説明

move コマンドを使用してファイルを移動します。

dest-directory を指定すると、ファイルは指定したフォルダに移動され、ファイル名は変更されません。

例

#ファイル flash:/test/sample.txt を flash:/に移動し、名前を 1.txt に変更します。

<Sysname> move test/sample.txt 1.txt

```
Move flash:/test/sample.txt to flash:/1.txt?[Y/N]:y
Moving file flash:/test/sample.txt to flash:/1.txt ... Done.
```

#ファイル b.cfg をフォルダ test2 に移動します。

<Sysname> move b.cfg test2

```
Move flash:/b.cfg to flash:/test2/b.cfg?[Y/N]:y
Moving file flash:/b.cfg to flash:/test 2/b.cfg ...Done.
```

6.1.14 pwd

Syntax

pwd

View

User view

定義済みユーザロール

network-admin

説明

pwd コマンドは、現在の作業パスを表示します。

例

#現在のパスを表示します。

<Sysname> pwd

```
flash:
```

6.1.15 rename

Syntax

rename { *source-file* | *source-directory* } { *dest-file* | *dest-directory* }

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file:ソースファイル名。

source-directory:ソースフォルダ名。

dest-file:ターゲットファイル名。

dest-directory:ターゲットフォルダ名。

説明

rename コマンドは、ファイルまたはフォルダの名前を変更します。

現在のパスにすでに存在するファイルまたは宛先フォルダと、宛先ファイル名または宛先フォルダが重複している場合(大文字と小文字は区別されず、同じ文字であれば同じ名前とみなされます。)、この操作は実行されません。

例

#ファイル名 copy.cfg を test.cfg に変更します。

<Sysname> rename copy.cfg test.cfg

```
Rename flash:/copy.cfg as flash:/test.cfg?[Y/N]:y
```

```
Renaming flash:/copy.cfg as flash:/test.cfg ...Done.
```

6.1.16 reset recycle-bin

Syntax

reset recycle-bin [**/force**]

View

User view

定義済みユーザロール

network-admin

パラメータ

/force:ごみ箱を直接空にするため、空にしたことをユーザが確認する必要はありません。このパラメータを指定しない場合、ごみ箱のパージ操作を実行すると、パージされる各ファイルが確認されます。

説明

reset recycle-bin コマンドを使用して、ごみ箱からファイルをパージします。

 注意

ごみ箱のファイルは、**undelete** コマンドを使用して復元できます。ごみ箱からファイルを削除すると、ファイルは復元できなくなります。このコマンドを実行する前に、ごみ箱のファイルがすべて無効であり、使用されないことを確認してください。

---

delete file コマンドを使用してファイルを削除すると、ごみ箱にファイルが格納されますが、ストレージ領域が消費されます。ごみ箱からファイルを削除するには、**reset recycle-bin** コマンドを実行する必要があります。

例

#ごみ箱にファイル a.cfg と b.cfg があるので、ごみ箱を空にします。

<Sysname> reset recycle-bin

```
Clear flash:/a.cfg?[Y/N]:y
Clearing file flash:/a.cfg ...Done.
Clear flash:/b.cfg?[Y/N]:y
Clearing file flash:/b.cfg ...Done.
```

#ごみ箱にファイル a.cfg と b.cfg があるので、b.cfg を削除します。

<Sysname> reset recycle-bin

```
Clear flash:/a.cfg?[Y/N]:n
```

```
Clear flash:/b.cfg?[Y/N]:y
Clearing file flash:/b.cfg ...Done.
```

関連コマンド

- **delete**

6.1.17 rmdir

Syntax

rmdir *directory*

View

User view

定義済みユーザロール

network-admin

パラメータ

directory:フォルダ名。

説明

rmdir コマンドは、フォルダを削除します。

注意

フォルダを削除する前に、フォルダ内のすべてのファイルとサブフォルダを完全に削除するか、一時的に削除する必要があります。ファイルが一時的に削除されただけの場合は、rmdir を実行すると、ごみ箱からファイルが完全に削除されます。この操作を行う前に、フォルダとその内容が使用されないことを確認してください。

例

#フォルダ subtest を削除します。

<Sysname> rmdir subtest/

```
Remove directory flash:/test/subtest and the files in the recycle-bin under
this directory will be deleted permanently.Continue?[Y/N]:y
Removing directory flash:/test/subtest ...Done.
```

6.1.18 tar create

Syntax

tar create [**gz**] **archive-file** *dest-file* [**verbose**] **source** { *source-file* | *source-directory* }&<1-5>

View

User view

定義済みユーザロール

network-admin

パラメータ

gz:パッケージ化後、パッケージファイルを gzip 形式で圧縮することを示します。このパラメータを指定しない場合は、パックのみで、圧縮は行われません。

archive-file dest-file:パッケージ化によって生成される新しいファイルの名前。gz パラメータを指定しない場合、dest-file のサフィックスは「.tar」である必要があります。gz パラメータを指定する場合、dest-file のサフィックスは「.tar.gz」である必要があります。

verbose:パッケージング中に、パッケージングされたファイルとフォルダの名前が 1 つずつ表示されます。このパラメータを指定しない場合、は表示されません。

source *{source-file |source-directory }&<1-5>*:現在のディレクトリにパッケージ化する必要があるソース/フォルダのリストを示します。フォルダを含めると、そのフォルダの下にあるすべてのファイルとサブフォルダがパッケージ化されます。&<1-5>は、前のパラメータが 5 回まで入力できることを示します。

説明

tar create コマンドは、複数のファイル/フォルダを 1 つの新しいファイルにパッケージ化するために使用します。

このコマンドを実行すると、デバイスは元のファイル/フォルダをコピーし、新しいファイルにパッケージ化して保存します。

例

#ファイル 1.cfg、2.cfg、および test をパッケージ化して、新しいファイル a.tar に保存します。

<Sysname> tar create archive-file a.tar source 1.cfg 2.cfg test
Creating archive flash:/a.tar Done.

#ファイル 1.cfg、2.cfg、および test をパッケージ化して新しいファイル b.tar.gz に保存します。

<Sysname> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test
Creating archive flash:/b.tar.gz Done.

#ファイル 1.cfg、2.cfg、およびフォルダ test をパックして新しいファイル c.tar.gz に保存し、パックされたファイルとフォルダの名前を 1 つずつ表示します。

<Sysname> tar create gz archive-file c.tar.gz verbose source 1.cfg 2.cfg test

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

関連コマンド

- **tar extract**
- **tar list**

6.1.19 tar extract

Syntax

tar extract archive-file *file* [**verbose**] [**screen** | **to** *directory*]

View

User view

定義済みユーザロール

network-admin

パラメータ

archive-file *file*:.tar または.tar.gz という接尾辞が付いた、解凍が必要なファイルの名前。

verbose:コマンドライン実行時に、file に含まれるすべてのファイル/フォルダの名前が表示されます。

screen:アンパックせず、file に含まれる元ファイルの内容のみを登録端末に出力する.テキストファイルのみを含む場合にはこのパラメータを用いることを提案する。

to *directory*:ターゲットパスに解凍します。directory は、アンパックされたファイルの保存パスです。

説明

tar extract コマンドを使用してファイルを解凍します。

screen パラメータを使用する前に、**tar list** コマンドを使用して圧縮パッケージ内のファイルのタイプを確認します。このパラメータは、テキストファイルのみを含める場合に推奨されます。圧縮パッケージにテキスト以外のファイルが含まれ、テキスト以外のファイルに端末制御文字が含まれている場合、screen パラメータを指定してこのコマンドを実行すると、現在のログイン端末の表示情報が文字化けしたり、現在のログイン端末が使用

できなくなったりすることがあります。通常は、現在の接続を切断してデバイスに再ログインすると、ログイン端末が通常の状態に戻ります。

screen および to directory パラメータを指定しない場合、ターゲットパスはユーザの現在のパスになります。

このコマンドを実行すると、デバイスは file に含まれるファイル/フォルダを解凍してから、名前を変更せずにターゲットパスに保存します。保存すると、保存先のパスにすでに存在する同じ名前のファイル/フォルダが自動的に上書きされます。

例

#a.tar を解凍します。

<Sysname> tar extract archive-file a.tar

```
Extracting archive flash:/a.tar Done.
```

#a.tar を解凍すると、a.tar に含まれるすべてのファイル/フォルダの名前が表示されます。

<Sysname> tar extract archive-file b.tar.gz verbose

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

#a.tar に含まれる元ファイルの内容を登録端末に直接出力する。

<Sysname> tar extract archive-file c.tar.gz screen

```
#
version 7.1.070、Release 1201
#
sysname Sysname
#
```

これらの操作を行うと、ファイルの内容が解凍されずに表示されます。残りのファイルの内容はここでは省略します。

関連コマンド

- **tar create**
- **tar list**

6.1.20 tar list

Syntax

tar list archive-file *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

archive-file file:表示するパッケージファイルの名前に.tar または.tar.gz という接尾辞が付きます。

説明

tar list コマンドは、パッケージファイルに含まれるファイル/フォルダの名前を表示します。

例

#a.tar に含まれるファイル/フォルダの名前を表示します。

<Sysname> tar list archive-file a.tar

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

関連コマンド

- **tar create**
- **tar extrac**

6.1.21 umount

Syntax

umount *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem:ファイルシステムの名前。

説明

umount コマンドを使用して、ファイルシステムをアンマウントします。

ストレージメディアをデバイスに接続すると、ファイルシステムはマウント状態で自動的にマウントされます。ユーザは、ストレージメディア上のすべてのファイルシステムをアンマウントしないと、ストレージメディアを安全に取り外すことができません。アンマウントすると、ファイルやストレージメディアが破損する可能性があります。

アンマウント操作中は、ファイルシステムの破損を防ぐために、ストレージメディアに対して次の操作を実行できません。

- ストレージメディアの抜き差しを禁止します。
- デバイスの再起動や電源オフを無効にします。
- 読み取り/書き込みのためにストレージメディアまたはストレージメディアにアクセスできないようにします。別のユーザがファイルシステムにアクセスしている場合は、umount 操作が失敗したことを示すメッセージが表示されます。

例

#USB ファイルシステムをアンマウントします。

<Sysname> umount usba0:

関連コマンド

- **mount**

6.1.22 undelete

Syntax

undelete *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file:リストアするファイルの名前。

説明

undelete コマンドを使用して、完全に削除されていない(ごみ箱に入れておきます)ファイルを復元します。復元されたファイル名が現在存在するファイルと重複している場合は、元のファイルを上書きするかどうかを確認するメッセージが表示されます。<Y>と入力すると、ソースファイルが上書きされます。<N>を入力すると、リカバリは実行されません。

例

#復元 flash:で削除されたファイル copy.cfg。

<Sysname> undelete copy.cfg

```
Undelete flash:/copy.cfg?[Y/N]:y
Undeleting file flash:/copy.cfg ...Done.
```

#flash:/seclog で削除されたファイル startup.cfg を復元します。

- 方法 1

<Sysname> undelete seclog/startup.cfg

```
Undelete flash:/seclog/startup.cfg?[Y/N]:y
Undeleting file flash:/seclog/startup.cfg ...Done.
```

- 方法 2

<Sysname> cd seclog

<Sysname> undelete startup.cfg

```
Undelete flash:/seclog/startup.cfg?[Y/N]:y
Undeleting file flash:/seclog/startup.cfg ...Done.
```

目次

このセクションのページは **2-x-x** です。

7 章 コンフィグレーションファイル管理 7-1
7.1 コンフィグレーションファイル管理コマンド 7-1
7.1.1 display current-configuration 7-1
7.1.2 display current-configuration diff 7-2
7.1.3 display default-configuration 7-4
7.1.4 display diff 7-5
7.1.5 display saved-configuration 7-7
7.1.6 display startup 7-8
7.1.7 display this 7-9
7.1.8 reset saved-configuration 7-10
7.1.9 save 7-11
7.1.10 standby auto-update config 7-13
7.1.11 startup saved-configuration 7-14

7章 コンフィグレーションファイル管理

7.1 コンフィグレーションファイル管理コマンド

7.1.1 display current-configuration

Syntax

display current-configuration [configuration [*module-name* **] | interface [** *interface-type* **[** *interface-number* **]]] [all]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

configuration [*module-name*]: 機能の設定を表示します。*module-name* 引数は機能モジュールを指定します。指定されない場合、設定されたすべての機能を表示します。有効な機能モジュールは装置の設定に依存します。

interface [*interface-type* [*interface-number*]]: インタフェースの設定を表示します。*interface-type* 引数はインタフェースタイプで、*interface-number* 引数はインタフェース番号を示します。

all:このキーワードを指定すると、このキーワードを指定しないときには表示されないすべてのカレントコンフィギュレーションを表示します。

説明

display current-configuration コマンドは現在の有効な設定を表示します。

本コマンドを使用して設定の確認を行うことができます。

simple 指定によるパスワード設定など、一部パラメータに対して行った設定がシステムによって自動的に変更された場合、このコマンドは、入力した設定ではなく変更された設定を表示します。通常、自動変更はシステムの制限などによって行われます。**all** キーワードを指定しない場合、このコマンドは一部の設定（主にデフォルト設定）を表示しません。

例

#ローカルユーザ設定を表示します。

<Sysname> display current-configuration configuration local-user

```
#
local-user ftp class manage
 password                                                                hash
$h$6$D5A6pqcGpnZXxFUO$OJqnqffG7m1wTH3C6v+FBCjZZBzqgJjTZlbATl1dnKNlYwFMJcWDMbD
n8HD1j4XzuKggDp2LrP40kGIOvQGYhQ==
 service-type ftp
 authorization-attribute user-role network-operator
#
local-user root class manage
 password                                                                hash
$h$6$GcTZyXO04qmom21z$GjeAeDMjP/xtknMLf9NHUNIvebNYR3tkd5aWS6sKbkFh/ECFJZOjh2F
VUI0GW7u44fNK6Ke7ANE7dhhAFcytUQ==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
return
```

VLAN インタフェース設定を表示します。

<Sysname> display current-configuration interface Vlan-interface

```
#
interface Vlan-interface1
 ip address 192.168.1.84 255.255.255
#
Return
```

7.1.2 display current-configuration diff

Syntax

display current-configuration diff

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display current-configuration diff コマンドは、次の起動プロファイルと実行プロファイルの違いを表示します。

次の起動プロファイルを他のプロファイルと比較する場合:

- 次回起動時のプロファイルの使用を優先します。
- プライマリの次回起動プロファイルが使用できない場合は、代替の次回起動プロファイルが使用されます。
- プライマリとスタンバイの両方の次回起動プロファイルが使用できない場合は、エラーメッセージが表示されます。

例

#次の起動プロファイルと実行プロファイルの違いを表示します。

<Sysname> display current-configuration diff

```
--- Startup configuration
+++ Current configuration
@@ -5, 7+5, 7 @@
#
sysname Sysname
#
-alias dhc display history-command
+alias dh display hotkey
```

<Sysname>

表 7-1 display current-configuration diff および display diff コマンドの表示情報の説明

フィールド	説明
---A +++ B	• Aは比較に関与するソースプロファイルを表し、Startup configuration、Current configuration、またはプロファイルの名前にすることができます。 • Bは比較対象のターゲットプロファイルを表し、Startup configuration、Current configuration、またはプロファイル名を指定できます。 この例では、Startup configurationは比較に関与するソースプロファイルを表し、Current configurationは比較に関与するターゲットプロファイルを表します。
@@-linenumber1、number1+linenumber2、number2@@	• -linenumber1, number1:Aの行番号linenumber1の構成から開始し、合計number1行を表示します。 • +linenumber2, number2:行番号linenumber2のB構成から開始し、合計number2行を表示することを示します。

フィールド	説明
cmd 1 -cmd 2 +cmd 3 cmd 4	• cmd 1、cmd 4は、AとBの両方に存在するコンフィギュレーションを表し、差分コンフィギュレーションのコンテキストは、差分コンフィギュレーションの場所を示します。 • -cmd 2は、構成がAの構成で、Bにはないことを示します。 • +cmd 3は、構成がBの構成で、Aにはないことを示します。 この例では、表示された情報から分かるように、alias dhc display history-commandはソースプロファイルにのみ存在し、alias dh display hotkeyはターゲットプロファイルにのみ存在するという違いがある。

関連コマンド

- **display current-configuration**
- **display diff**
- **display saved-configuration**

7.1.3 display default-configuration

Syntax

display default-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display default-configuration コマンドは、デバイスの工場出荷時の設定を表示するために使用されます。

デバイスは通常、出荷時に出荷時構成と呼ばれる基本的な構成で出荷されます。これは、設定ファイルがない場合や、設定ファイルが破損している場合に、デバイスが正常に起動して動作することを保証するために使用されます。

出荷時の構成がコマンドラインのデフォルトと一致しない場合があります。デバイスは必要に応じて出荷時の構成をカスタマイズします。

デバイスが工場出荷時の設定にカスタマイズされていない場合、このコマンドは空白になります。

例

#デバイスの工場出荷時の設定を表示します。

<Sysname> display default-configuration

7.1.4 display diff

Syntax

display diff configfile *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** }

display diff current-configuration { **configfile** *file-name-d* | **startup-configuration** }

display diff startup-configuration { **configfile** *file-name-d* | **current-configuration** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

configfile *file-name-s*:比較に使用するソースプロファイルを指定します。file-name-s は設定ファイルの名前です。

configfile *file-name-d*:比較に使用するターゲットプロファイルを指定します。file-name-d は設定ファイルの名前です。

current-configuration: 現在実行中の設定を示します。**display diff current-configuration** コマンドでは、このキーワードは、比較に参加するように現在実行が設定されているソース設定を示します。**display diff configfile file-name-s** コマンドおよび **display diff startup-configuration** コマンドでは、このキーワードは、比較に関与するように現在実行が設定されているターゲット設定を示します。

startup-configuration:プロファイルが次に起動されることを示します。**display diff startup-configuration** コマンドでは、このキーワードは、次の起動プロファイルが比較に関与するソースプロファイルであることを示します。このキーワードは、**display diff configfile file-name-s** コマンドと **display diff current-configuration** コマンドで、次の起動プロファイルが比較対象のターゲットプロファイルであることを示します。

説明

display diff コマンドを使用すると、2 つの設定の違いを確認できます。

次の起動プロファイルを他のプロファイルと比較する場合:

- 次回起動時のプロファイルの使用を優先します。
- プライマリの次回起動プロファイルが使用できない場合は、代替の次回起動プロファイルが使用されます。
- プライマリとスタンバイの両方の次回起動プロファイルが使用できない場合は、エラーメッセージが表示されます。

例

#プロファイル startup.cfg と test.cfg の違いを表示します。

<Sysname> display diff configfile startup.cfg configfile test.cfg

```
--- flash:/startup.cfg
+++ flash:/test.cfg
@@ -5, 7+5, 7 @@
#
sysname Sysname
#
-alias dhc display history-command
+alias dh display hotkey
```

<Sysname>

上記の情報は、startup.cfg ファイルに設定 alias dhc display history-command があり、test.cfg ファイルに設定 alias dh display hotkey があることを示しています。

#実行構成と次回起動構成ファイルの違いを表示します。

<Sysname> display diff current-configuration startup-configuration

```
--- Current configuration
+++ Startup configuration
@@ -5, 7+5, 7 @@
#
sysname Sysname
#
-alias dhc display history-command
+alias dh display hotkey
```

<Sysname>

上記の情報は、実行コンフィギュレーションに alias dhc display history-command があり、次のスタートアップコンフィギュレーションファイルに alias dh display hotkey があることを示しています。

このコマンドで表示される情報の説明については、表 7-1 を参照してください。

関連コマンド

- **display current-configuration**
- **display current-configuration diff**
- **display saved-configuration**

7.1.5 display saved-configuration

Syntax

display saved-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display saved-configuration コマンドは、次回の起動プロファイルの内容を表示するために使用します。

このコマンドを使用すると、デバイスの管理/メンテナンス時に、重要な構成が次の起動プロファイルに保存されていることを確認できます。

次回起動時にプロファイルの内容を確認する場合:

- マスター次回起動プロファイルが存在する場合、このコマンドを実行すると、マスター次回起動プロファイルの内容が表示されます。
- プライマリ次回起動プロファイルが存在せず、スタンバイ次回起動プロファイルが存在する場合、このコマンドを実行すると、スタンバイ次回起動プロファイルの内容が表示されます。
- プライマリとスタンバイの両方の次回起動プロファイルが存在しない場合、このコマンドを実行しても情報は表示されません。

例

#メインの次回起動プロファイルの内容を表示します。

<Sysname> display saved-configuration

```
#
 version 9.2.01
#
 sysname Sysname
#
 ftp server enable
#
 telnet server enable
#
 domain default enable system
#
vlan 1
#
```

```
domain system
#
  ---- More ----
```

関連コマンド

- **reset saved-configuration**
- **save**

7.1.6 display startup

Syntax

display startup

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display startup コマンドは、今回および次回の起動に使用するプロファイルの名前を表示します。

例

#今回および次回起動するプロファイル名を表示します。

<Sysname> display startup

```
Current startup saved-configuration file:flash:/startup.cfg (*)
Next main startup saved-configuration file:flash:/startup.cfg
Next backup startup saved-configuration file:NULL
```

表 7-2 display startup コマンドの表示情報の説明

フィールド	説明
Current Startup saved-configuration file	現在の起動で使用されているプロファイル このフィールドの後に 「*」 が付いている場合は、現在の起動プロファイルがバイナリタイプであることを示します。
Next main startup saved-configuration file	次回起動時に使用するマスタープロファイル
Next backup startup saved-configuration file	次回の起動時に使用する代替プロファイル

関連コマンド

- **startup saved-configuration**

7.1.7 display this

Syntax

display this［ **all** ］

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:現在のビューのすべての構成情報を表示します。このパラメータを指定しない場合、デフォルト以外の構成情報のみが表示されます。

説明

display this コマンドは、現在のビューで有効な設定を表示します。

ユーザがビューで一連の構成を完了した後、構成が正常に完了したことを確認する必要がある場合は、**display this** コマンドを実行して、現在有効な構成を表示できます。

パラメータ all が指定されていない場合、すでに有効になっている構成の一部は、デフォルトと同じであれば表示されません。

一部のパラメータでは、ユーザが設定されていても、その機能が有効になっていない場合は表示されません。

いずれかのユーザインタフェースビューでこのコマンドを実行すると、すべてのユーザ線で有効な設定が表示されます。

例

#インタフェース Vlan-interface1 で有効な設定を表示します。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] display this
#
interface Vlan-interface1
#
return
```

7.1.8 reset saved-configuration

Syntax

reset saved-configuration [**backup** | **main**]

View

User view

定義済みユーザロール

network-admin

パラメータ

backup:スタンバイ次回起動プロファイルを削除します。

main:マスターを削除して次にプロファイルを起動します。

説明

reset saved-configuration コマンドは、デバイスのストレージメディアに保存されている次の起動プロファイルを削除します。

 注意

このコマンドを実行すると、デバイスからプロファイルが完全に削除されます。このコマンドは慎重に使用してください。

この機能を使用すると、ユーザが現在のシステムで指定されている次回起動プロファイルを使用してデバイスを起動しなくなったときに、次回起動プロファイルをデバイスから削除できます。

アプライアンスのプライマリスタンバイの次回起動プロファイルが同じで、削除操作が 1 回だけ実行された場合(たとえば、backup パラメータを指定します。)、対応する次回起動プロファイルのみが NULL に設定され、ファイルは削除されません。プロファイルを完全に削除するには、削除操作を再度実行する必要があります(main パラメータの指定)。

backup パラメータと main パラメータを指定しない場合、デフォルトで main が使用されます。

例

#次の起動プロファイルを使用してマスターを削除します。

<Sysname> reset saved-configuration

```
The saved configuration file will be erased.Are you sure?[Y/N]:y
Configuration file in flash:is being cleared.
Please wait ..........
Configuration file is cleared.
```

関連コマンド

- **display saved-configuration**

7.1.9 save

Syntax

save *file-url*

save [**safely**] [**backup** | **main**] [**force**] [**changed**]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

file-url:ファイルパス。ファイル名の部分にはサフィックス「.cfg」を付ける必要があり、ファイルパスの合計は 255 文字を超えることはできません。

safely:設定ファイルをセーフモードで保存します。このパラメータを指定しない場合、構成ファイルは簡易保存で保存されます。

backup:このファイルを代替の次回起動プロファイルに設定します。backup と main を指定しない場合は、デフォルトで main が使用されます。

main:このファイルをメインの次回起動プロファイルに設定します。backup と main を指定しない場合は、デフォルトで main が使用されます。

force:現在の構成をマスターの次回起動時に直接保存すると、システムは対話型情報を出力しなくなります。デフォルトでは、ユーザは save コマンドを実行し、ユーザは<Y>や<N>などのパラメータを入力してこの操作を確認する必要があります。30 秒以内に確認されない場合、システムは自動的にこの操作を終了します。save オペレーションの実行時に force パラメータを使用した場合、現在の構成は直接保存され、ユーザ入力は不要になります。

changed:現在の実行コンフィギュレーションがターゲットプロファイルと比較して変更されている場合は、現在のコンフィギュレーションをデバイスターゲットプロファイルに保存します。それ以外の場合は、コンフィギュレーションの保存は実行されません。このパラメータを指定しない場合、構成が変更されたかどうかに関係なく、構成の保存操作が実行されます。

説明

save file-url コマンドは、デバイスの現在の構成をファイルに保存するために使用されますが、このファイルは次回起動時に設定されません。

save [safely] [backup |main] [force] [changed]コマンドを使用して、現在のコンフィギュレーションをストレージメディアのルートディレクトリに保存し、そのファイルを次回のスタートアップコンフィギュレーションファイルに設定します。

⚠ 注意

save コマンドを実行すると、既存の構成ファイルが上書きされる可能性があります。デバイスのプロンプトに注意してください。

---

save コマンドの実行時に指定したファイル名が存在しない場合は、保存操作を実行する前にファイルが作成されます。指定したファイル名が存在する場合、そのファイルを上書きするかどうかを確認するメッセージが表示されます。上書きしないことを選択した場合、**save** コマンドは続行されません。

save コマンドの実行時に file-url パラメータを指定しない場合、デバイスは現在の構成をストレージメディアのルートディレクトリに保存し、このファイルを次回の起動時の構成ファイルに設定します。file-url パラメータを指定すると、デバイスは現在の構成のみを指定したファイルに保存します。

ユーザが **save** コマンドを実行して構成を保存すると、テキスト型の構成ファイル(「.cfg」というサフィックスが付いており、**more** コマンドでファイルの内容を確認できる)とバイナリ型の構成ファイル(サフィックスは「.mdb」です。このプロファイルはソフトウェアのみが解決でき、ユーザはファイルの内容を読み取り、編集できません。)が自動的に生成されるが、 2 つのファイルの内容はまったく同じであり、デバイスの起動時にバイナリ型の構成ファイルを優先的に使用することで、構成のロード速度を向上させている。バイナリ・タイプの構成ファイルがない場合は、テキスト・タイプの構成ファイルが使用されます。

save [safely] [backup |main] [force] [changed]コマンドを実行して、デバイス上にすでに存在するファイルと同じ名前のファイル名を入力した場合:

- safely パラメータを使用すると、現在の構成が一時ファイルに保存されます。保存に成功すると、同じ名前のファイルが一時ファイルに置き換えられます。このため、保存中に機器の再起動や電源オフなどのトラブルが発生して構成の保存に失敗しても、同じ名前の構成ファイルで機器を起動できる。
- safely パラメータを使用しない場合、同じ名前の元のファイルが直接上書きされます。保存中にデバイスの再起動、電源切断、メモリ不足、デバイスのストレージスペース不足などの問題が発生した場合、結果は現在の構成の保存に失敗し、元の同名ファイルは削除され、次の起動ファイルは空になります。

したがって、セキュリティ上の理由から、現在の設定を次回の起動プロファイルに保存する必要がある場合は、safely パラメータを使用することをお勧めします。

例

#現在のプロファイルをプロファイル backup.cfg に保存しますが、次回の起動プロファイルには設定しません。

<Sysname> save backup.cfg

```
The current configuration will be saved to flash:/backup.cfg.Continue?[Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/backup.cfg.Please wait ...
Configuration is saved to device successfully.
```

#現在の設定をメインの次回起動時に設定ファイルに直接保存します。

<Sysname> save force

```
Validating file.Please wait ....
Saved the current configuration to mainboard device successfully.
```

#現在の構成をストレージメディアのルートディレクトリに保存し、次回起動時の構成ファイルに設定します。

<Sysname> save

```
The current configuration will be written to the device.Are you sure?[Y/N]:y
Please input the file name (*.cfg) [flash:/backup.cfg]
(To leave the existing filename unchanged、press the enter key):test.cfg
Validating file.Please wait ............
Saved the current configuration to mainboard device successfully.
```

関連コマンド

- **display current-configuration**
- **display saved-configuration**

7.1.10 standby auto-update config

Syntax

standby auto-update config

undo standby auto-update config

デフォルト

次回起動時の設定ファイル操作は、システム全体で自動的に同期されます。

View

System view

定義済みユーザロール

network-admin

説明

システム全体の次スタートアップコンフィギュレーションファイルの自動操作を有効にするには、**standby auto-update config** コマンドを使用します。

システム全体の次スタートアップコンフィギュレーションファイルの自動操作を無効にするには、**undo standby auto-update config** コマンドを使用します。

デフォルトでは、システム全体の自動次スタートアップコンフィギュレーションファイル操作が有効になっています。システムは、マスタデバイスに加えて、すべてのクラウドクラスタスタンバイデバイスで次の操作を実行します。

- **save** [**safety**] [**backup**|**main**] [**force**] [**changed**] コマンドを実行すると、実行コンフィギュレーションが各メンバーデバイスの次スタートアップコンフィギュレーションファイルに保存されます。
- **reset saved-configuration** コマンドを実行すると、各メンバーデバイスの次スタートアップコンフィギュレーションファイルが削除されます。

システム全体の次のスタートアップコンフィギュレーションファイルの自動操作を無効にすると、システムは実行コンフィギュレーションを保存するか、マスタデバイスだけの次のスタートアップコンフィギュレーションファイルを削除します。

システム全体の自動操作により、マスタデバイスとスタンバイデバイス間のスタートアップコンフィギュレーションファイルの一貫性が保証されます。ただし、システム全体の操作は、マスタデバイスだけで実行される操作よりも時間がかかります。また、システム全体の構成操作を完了するために必要な時間は、構成データの量が増えるにつれて増加します。

構成の保存を高速化するためにシステム全体の自動操作を無効にしている場合は、マスタデバイスとスタンバイデバイスの間で次のスタートアップ構成ファイルが不整合になることに注意してください。

例

```
# システム全体で自動的にコンフィグファイルを同期する設定を有効にします。
<Sysname> system-view
[Sysname] standby auto-update config
```

関連コマンド

- **reset saved-configuration**
- **save**

7.1.11 startup saved-configuration

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

デフォルト

次の起動プロファイルが設定されていません。

View

User view

定義済みユーザロール

network-admin

パラメータ

cfgfile:構成ファイルのパス、およびファイル名。このファイルは、ストレージメディアのルートディレクトリにある.cfg サフィックスを含むファイルであり、255 文字以内で指定する必要があります。このパラメータは、プロファイル名、またはストレージメディア名+プロファイル名のみです。

backup:プロファイルを代替の次回起動プロファイルに設定します。

main:プロファイルをマスターに設定し、次にプロファイルを起動します。デバイスは、プライマリ次回起動プロファイルを優先的に使用し、プライマリ次回起動プロファイルが存在しないか破損している場合は、スタンバイ次回起動プロファイルを使用します。

説明

startup saved-configuration コマンドを使用して、次の起動プロファイル(システムの次回起動時に使用する構成ファイル)を設定します。

undo startup saved-configuration コマンドは、工場出荷時の設定で起動するようにデバイスを設定するために使用します。

main パラメータと backup パラメータを指定しない場合、デフォルトで main が使用されます。

プライマリ次回起動プロファイルとスタンバイ次回起動プロファイルは同じファイルに設定できますが、信頼性を高めるために、異なるファイルに設定するか、1 つのプロファイルをプライマリとスタンバイの 2 つの異なる名前のファイルに保存することをお勧めします。

undo startup saved-configuration コマンドを実行すると、プライマリ/スタンバイの次回起動プロファイルは NULL に設定されますが、ファイルは削除されません。

save コマンドを実行すると、現在のプロファイルがストレージメディアに保存され、次回の起動時に使用するプライマリまたはスタンバイプロファイルに設定されます。

例

#次の起動プロファイルを設定します。

<Sysname> startup saved-configuration testcfg.cfg

```
Please wait .......Done.
```

関連コマンド

display startup

目次

このセクションのページは **2-x-x** です。

8 章 ソフトウェアのアップグレード 8-1
8.1 ソフトウェアアップグレード構成コマンド 8-1
8.1.1 boot-loader file 8-1
8.1.2 display boot-loader 8-3
8.1.3 display version 8-4

8章 ソフトウェアのアップグレード

8.1 ソフトウェアアップグレード構成コマンド

8.1.1 boot-loader file

Syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*&<*1-30*>] [**patch** *filename*&<*1-30*>] { **backup** | **main** }

boot-loader file *ipe-filename* { **all** | **slot** *slot-number* } { **backup** | **main** }

View

User view

定義済みユーザロール

network-admin

パラメータ

boot:Boot パッケージ。

system:System パッケージ。

feature:Feature パッケージ。

patch:最大 30 個のインクリメンタルパッチイメージファイルまたは 16 個の非インクリメンタルパッチイメージファイルのスペース区切りリストを指定します。ブートイメージ、システムイメージ、および機能イメージはそれぞれ非インクリメンタルパッチイメージファイルを 1 つ持つことができるため、最大 16 個の非インクリメンタルパッチイメージファイルを指定できます。

filename& <1-30>:filesystemname/filename.bin のようなパッケージの名前。このファイルは、デバイスのいずれかのファイルシステムのルート・ディレクトリに保存する必要があります。このパラメータには、ファイルシステムの名前を格納メディア名から 63 文字以内で入力します。&<1-30>は、前のパラメータが最大 30 回入力できることを示します。

ipe-filename:filesystemname/filename.ipe のような IPE (Image Package Envelope、複合パッケージスイート)ファイルの名前。このファイルは、デバイスのいずれかのファイルシステムのルート・ディレクトリに保存する必要があります。このパラメータには、ファイルシステムの名前を格納メディア名から 63 文字以内で入力します。

フォルダとファイルを指定する方法については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*10 章 ファイルシステム管理*”を参照してください。

all:クラウドクラスタのメンバ装置に対してスタートアップイメージを指定します。このパラメータを指定した場合、クラウドクラスタのすべてのメンバ装置をアップグレードします。

slot: *slot-number*: クラウドクラスタのメンバ装置のメンバ ID を指定します。

backup:このパッケージを代替起動パッケージとして指定します。代替起動パッケージ:プライマリ起動パッケージが使用できない場合や、例外が発生した場合に起動デバイスを起動します。

main:パッケージがマスター起動パッケージであることを指定します。マスター起動パッケージは、デバイスの起動に使用されます。

説明

boot-loader file コマンドは、デバイスが次回起動するときに使用するパッケージを設定します。

 注意

このコマンドが正常に実行されると、システムは、既存のパッケージリストをコマンドで指定されたパッケージに置き換える前に、パッケージをデジタル署名付きで検証します。検証に成功すると、既存のパッケージリストが置き換えられます。パッケージが検証に失敗した場合、既存のパッケージリストは置き換えられず、エラーメッセージが返されます。

コマンドが正常に実行されると、既存のパッケージリストがコマンドで指定されたパッケージに置き換えられます。コマンドラインで Feature パッケージが指定されていない場合、Feature パッケージは更新されたパッケージリストに表示されません。

指定された次回起動パッケージのロードを完了するには、システムを再起動する必要があります。

例

#デバイスの次回起動時に使用するマスター起動ファイルを flash:/all.ipe に設定します。

<Sysname> boot-loader file flash:/all.ipe main

```
Verifying the file flash:/all.ipe on the device ..... Done.
QX-W2300AC シリーズ images in IPE:
boot.bin
system.bin
This command will set the main startup software images.Continue?[Y/N]:Y
Add images to the device.
File flash:/boot.bin already exists on the device.
File flash:/system.bin already exists on the device.
Overwrite the existing files?[Y/N]:Y
Decompressing file boot.bin to flash:/boot.bin ..... Done.
```

```
Decompressing file system.bin to
flash:/system.bin ............................. Done.
Verifying the file flash:/boot.bin on the device ... Done.
Verifying the file flash:/system.bin on the device ............. Done.
The images that have passed all examinations will be used as the main startup
software images at the next reboot on the device..
```

#デバイスの次回起動時に使用するマスター起動ファイルを flash:/boot.bin および flash:/system.bin に設定します。

<Sysname> boot-loader file boot flash:/boot.bin system flash:/system.bin main

```
This command will set the main startup software images.Continue?[Y/N]:y
The images that have passed all examinations will be used as the main startup
software images at the next reboot on the device.
```

関連コマンド

- **display boot-loader**

8.1.2 display boot-loader

Syntax

display boot-loader

View

すべてのビュー

定義済みユーザロール

network-admin

network-operator

説明

display boot-loader コマンドは、この起動と次の起動に使用する起動パッケージの名前を表示します。

例

#今回の起動と次回の起動で使用する起動パッケージの名前を表示します。

<Sysname> display boot-loader

```
Software images on the device:
Current software images:
flash:/boot.bin
flash:/system.bin
Main startup software images:
flash:/boot.bin
flash:/system.bin
```

```
Backup startup software images:
flash:/boot.bin
flash:/system.bin
```

#今回の起動と次回の起動で使用する起動パッケージの名前を表示します。

<Sysname> display boot-loader

```
Software images on the device:
Current software images:
  Image              Version
  flash:/boot.bin      Release 0053
  flash:/system.bin    Release 0053
Main startup software images:
  Image              Version
  flash:/boot.bin      Releae 0054
  flash:/system.bin    Releae 0054
Backup startup software images:
  Image              Version
  flash:/b-boot.bin    --
  flash:/b-system.bin   --
```

表 8-1 display boot-loader コマンドの表示情報の説明

フィールド	説明
Current software images	前回の起動時に使用した起動パッケージの一覧
Main startup software images	次回起動パッケージリストのマスター
Image	イメージ名
Version	イメージバージョン。 イメージが破損または削除された場合、このフィールドには2つのハイフン (--) が表示されます。
Backup startup software images	スタンバイ次回起動パッケージリスト

関連コマンド

- **boot-loader file**

8.1.3 display version

Syntax

display version

View

すべてのビュー

定義済みユーザロール

network-admin

network-operator

説明

display version コマンドを使用して、システムのバージョン情報を表示します。

例

#システムのバージョン情報を表示します。

<Sysname> display version

```
Comware Software, Version 9.1.01
QX-W2300AC シリーズ uptime is 0 weeks, 6 days, 20 hours, 37 minutes
Last reboot reason : User soft reboot

Boot image: flash:/boot.bin
Boot image version: 9.1.01
  Compiled May 26 2020 14:00:00
System image: flash:/system.bin
System image version: 9.1.01
  Compiled May 26 2020 14:00:00

...
```

表 8-2 display version コマンドの表示情報の説明

フィールド	説明
Last reboot reason	デバイスが最後に再起動した理由を示します。主な値は次のとおりです。 ● User soft reboot:ユーザーがコマンドライン、SNMPなどを使用してデバイスを再起動したことを示します。 ● Power on:停電による再起動を示す ● Kernel exception soft reboot:カーネルの異常による再起動を示します ● Kernel deadloop soft reboot:　再起動はカーネルスレッドのデッドループによって発生しました。 ● Dev Hand Shake soft reboot:デバイス管理ハンドシェイクの失敗による再起動を示します。 ● Auto update soft reboot:バージョンの自動アップグレードによる再起動を示します。 ● Memory exhaust reboot:シングルボードメモリ不足による再起動を示します。 ● Critical process abnormality reboot:クリティカルプロセスの例外による再起動を示します。

目次

このセクションのページは **2-x-x** です。

9 章 Python 9-1
9.1 Python 設定コマンド 9-1
9.1.1 exit() 9-1
9.1.2 python 9-1
9.1.3 python filename 9-2

9章 Python

9.1 Python設定コマンド

9.1.1 exit()

Syntax

exit ()

View

Python shell

定義済みユーザロール

network-admin

説明

exit ()コマンドを使用して、Python shell を終了します。

Python shell で quit コマンドを使用して終了することはできません。exit ()コマンドを実行して、Python shell からユーザビューに戻ることができます。

例

#Python shell を終了します。

```
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright"、 "credits" or "license" for more information.
>>>
>>>exit ()
<Sysname>
```

9.1.2 python

Syntax

python

View

ユーザビュー

定義済みユーザロール

network-admin

説明

python コマンドは Python shell に入るのに使用されます。

Python shell にアクセスすると、バージョン Python2.7 のコマンドと標準 API、または Comware V9 の拡張 API を使用できます。

例

#Python shell に入ります。

<Sysname> python

```
Python 2.7.3 (default)
[GCC 6.2.0] on linux2
Type "copyright"、 "credits" or "license" for more information.
>>>
```

9.1.3 python filename

Syntax

python *filename* [*param*]

View

ユーザビュー

定義済みユーザロール

network-admin

パラメータ

filename:Python スクリプトファイルの名前。このファイルは、デバイスファイルシステムに存在するファイルである必要があります。ファイル名は大文字と小文字を区別し、拡張子は「.py」である必要があります。拡張子は大文字と小文字を区別しません。

param:Python スクリプトファイルの実行時に指定されたパラメータ。複数のパラメータはスペースで区切られます。

説明

python filename コマンドは、Python スクリプトファイルを実行するために使用します。スクリプトの実行中は、現在ログオンしているユーザーは他のアクションを実行できません。他のアクションを実行するには、スクリプトの実行が完了するまで待つ必要があります。

スクリプト構文が正しいことを確認してください。スクリプト内のディレクティブに構文エラーがあることが検出されると、そのディレクティブとそれ以降のディレクティブは実行されなくなります。

システムがスクリプト内の対話型ディレクティブを実行すると、デフォルト値を使用して実行が継続されます。

例

#Python スクリプトファイル test.py を実行します。

<Sysname> python test.py 1 2

```
['/flash:/test.py'、'1'、'2']
```

目次

このセクションのページは **2-x-x** です。

10 章 Tcl 10-1
10.1 Tcl 設定コマンド 10-1
10.1.1 cli 10-1
10.1.2 tclquit 10-2
10.1.3 tclsh 10-2

10章 Tcl

10.1 Tcl設定コマンド

10.1.1 cli

Syntax

cli *command*

View

Tcl 構成ビュー

定義済みユーザロール

network-admin

パラメータ

command:実行する必要がある **Comware** コマンド。**Comware** コマンドとして完全なコマンドラインを入力します。

説明

cli コマンドは、Tcl 構成ビューで **Comware** コマンドを優先的に実行するために使用されます。

Tcl 設定ビューでコマンドを実行する場合、**Tcl** コマンドが **Comware** コマンドのコマンドワードと競合すると、**Tcl** コマンドが実行されます。Tcl 設定ビューで **Comware** コマンドを優先する必要がある場合は、**Comware** コマンドの前に **cli** というコマンドキーワードを追加できます。

例

#Tcl 設定ビューで次に複数の Comware コマンドを実行して下さい:

<Sysname> tclsh

<Sysname-tcl> system-view

- 方式 1:

[Sysname-tcl] cli "vlan 2 ;description Tech"

- 方式 2:

[Sysname-tcl] cli vlan 2 ;cli description Tech

10.1.2 tclquit

Syntax

tclquit

View

Tcl 構成ビュー

定義済みユーザロール

network-admin

説明

tclquit コマンドは、Tcl 設定ビューからユーザビューに戻るために使用します。

このコマンドを実行することは、Tcl 構成ビューで **quit** コマンドを実行することと同じです。

Tcl 構成ビューで **Comware** コマンドを使用して子ビューに移動した場合は、**quit** コマンドを使用して前のレベルのビューに戻るだけで、**tclquit** コマンドは実行できません。

例

#Tcl 設定ビューからユーザビューに戻ります。

<Sysname-tcl> tclquit

<Sysname>

関連コマンド

- tclsh

10.1.3 tclsh

Syntax

tclsh

View

ユーザビュー

定義済みユーザロール

network-admin

説明

tclsh コマンドを使用して、ユーザビューから Tcl 設定ビューに移動します。

Comware 設定と互換性を持たせるために、Tcl 設定ビューの下で、ユーザは次のコマンドを直接入力して、直接入力することができます。

- すべてのバージョン Tcl8.5 のコマンド。
- Comware システムのコマンド。Tcl 設定ビューはユーザビューに相当し、ユーザビューの下の設定と同じように設定されます。

例

#ユーザビューから Tcl 設定ビューに移動します。

<Sysname> tclsh

<Sysname-tcl>

関連コマンド

- tclquit

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

3. システム管理

本マニュアルは以下に示す章で構成されています。

01- 装置管理

02- 装置ハードニング

03- ハードウェアリソース管理

04- NTP

05- Information Center

目次

このセクションのページは **3-x-x** です。

1 章 装置管理 1-1
1.1 装置管理コマンド 1-1
1.1.1 clock datetime 1-1
1.1.2 clock protocol 1-2
1.1.3 clock summer-time 1-3
1.1.4 clock timezone 1-5
1.1.5 command 1-6
1.1.6 copyright-info enable 1-7
1.1.7 diag boot-info display 1-8
1.1.8 display clock 1-11
1.1.9 display diagnostic-information 1-12
1.1.10 display scheduler job 1-15
1.1.11 display scheduler logfile 1-15
1.1.12 display scheduler reboot 1-17
1.1.13 display scheduler schedule 1-17
1.1.14 header 1-19
1.1.15 job 1-20
1.1.16 locator blink 1-21
1.1.17 reboot 1-22
1.1.18 reset scheduler logfile 1-24
1.1.19 restore factory default 1-24
1.1.20 scheduler job 1-25
1.1.21 scheduler logfile size 1-26
1.1.22 scheduler reboot at 1-27
1.1.23 scheduler reboot delay 1-28
1.1.24 scheduler schedule 1-29
1.1.25 sysname 1-30
1.1.26 time at 1-31
1.1.27 time once 1-32
1.1.28 time repeating 1-34
1.1.29 user-role 1-36

1章 装置管理

1.1 装置管理コマンド

1.1.1 clock datetime

Syntax

clock datetime *time date*

デフォルト

システム時刻は UTC の 2011 年 1 月 1 日 0 時です。

View

User View

定義済みユーザロール

network-admin

パラメータ

time:HH:MM:SS (時間:分:秒)形式で設定された時刻。HH は 0~23 の範囲で指定し、MM および SS は 0~59 の範囲で指定します。整数に設定する場合は、秒を入力しないでください。整数を設定する場合は、分と秒を入力しないでください。たとえば、 time 変数を 0 に設定すると零点を表す。

date:MM/DD/YYYY (月/日/年)または YYYY/MM/DD (年/月/日)の形式で構成された日付。MM は 1~12、DD は月、YYYY は 2000~2035 の範囲で値を指定できます。

説明

clock datetime コマンドを使用して、デバイスのシステム時刻を設定します。

 注意

このコマンドを実行すると、デバイスのシステム時間が変更され、システム時間に関連する機能(たとえば、タスクのスケジュール設定機能)の実行や、他のデバイスとの連携(たとえば、ログのエスカレーションと統計)に影響を及ぼす可能性があります。

他の装置との協調動作を保証し、装置をよりよく監視し、維持するために、装置のシステム時間が正確であることを確認してください。

このコマンドを実行する前に、**clock protocol none** コマンドを設定してください。**clock datetime** コマンドで指定した時刻は、現在のシステム時刻として即時に有効になります。その後、装置は内部結晶振動器が生成するクロック信号を使用して計時する。

デバイスの電源をオフにして再起動すると、コマンドはデフォルトに戻り、再構成が必要になります。

例

#設定アプライアンスのシステム時刻は 2019 年 1 月 1 日 8:08:08 です。

<AC> clock datetime 8:8:8 1/1/2019

#設定アプライアンスのシステム時刻は 2019 年 1 月 1 日 8:10 です。

<AC> clock datetime 8:10 2019/1/1

関連コマンド

- **clock protocol**
- **clock summer-time**
- **clock timezone**
- **display clock**

1.1.2 clock protocol

Syntax

clock protocol { **none** | **ntp** }

undo clock protocol

デフォルト

NTP プロトコルを使用して時刻を取得します。

View

System view

定義済みユーザロール

network-admin

パラメータ

none:システム時刻がコマンドラインから設定されていることを示します。

ntp:NTP (Network Time Protocol、ネットワークタイムプロトコル)プロトコルを介して時刻を取得することを示します。NTP の詳細および構成は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*4 章 NTP*”を参照してください。

説明

clock protocol コマンドは、システム時刻の取得方法を設定します。

undo clock protocol コマンドを使用して、デフォルトの状態を復元します。

他の装置との協調動作を保証し、装置をよりよく監視し、維持するために、装置のシステム時間が正確であることを確認してください。

システム時刻の取得方法は次のとおりです。

- **clock protocol none** コマンドを設定したら、**clock datetime** コマンドを使用して直接設定します。**clock datetime** コマンドで指定した時刻が、現在のシステム時刻になります。その後、装置は内部結晶振動器が生成するクロック信号を使用して計時する。
- **clock protocol {ntp}**コマンドを設定した後、NTP プロトコルを使用してネットワークから時刻を取得します。この方法では、デバイスは定期的にサーバの UTC (Coordinated Universal Time、協定世界時)時刻を同期し、同期した UTC 時刻とデバイスに設定されているローカルタイムゾーン、夏時間パラメータを使用して現在のシステム時刻を計算します。この方法は、コマンドラインで設定された時間よりも正確な時間を取得します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#設定 UTC 時刻を取得する方法は、コマンドラインで設定します。

<AC> system-view

[AC] clock protocol none

1.1.3 clock summer-time

Syntax

clock summer-time *name start-time start-date end-time end-date add-time*

undo clock summer-time

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

name:夏時間の名前。1~32 文字の文字列で、大文字と小文字が区別されます。

start-time:開始時間。HH:MM:SS 形式で、HH は 0~23 の範囲で値を指定し、MM および SS は 0~59 の範囲で値を指定します。整数に設定する場合は、秒を入力しないでください。整数を設定する場合は、分と秒を入力しないでください。

start-date:開始日には、次の 2 つの入力方法があります。

- 月と日を一度に入力します。パラメータの形式は MM/DD、MM の範囲は 1~12、DD の範囲は月に関連します。
- 月、日を入力します。パラメータ間は<スペース>キーで区切ります。最初に、January、February、March、April、May、June、July、August、September、October、November、または December の開始月を入力します。次に、開始週を入力し、その月の何週目かを first、January、February、March、April、または last で指定します。最後に、August、September、October、November、December、first、または January の開始日を入力します。

end-time:終了時間。HH:MM:SS の形式で、HH は 0~23 の範囲で、MM および SS は 0~59 の範囲で値を指定します。整数に設定する場合は、秒を入力しないでください。整数を設定する場合は、分と秒を入力しないでください。

end-date:終了日には、次の 2 つの入力方法があります。

- 月の日を一度に直接入力します。パラメータの形式は MM/DD、MM の範囲は 1~12、DD の範囲は月に関連します。
- 月、日を入力します。パラメータ間は<スペース>キーで区切ります。最初に、January、February、March、April、May、June、July、August、September、October、November、または December の開始月を入力します。次に、開始週を入力し、その月の何週目かを first、January、February、March、April、または last で指定します。最後に、August、September、October、November、December、first、または January の開始日を入力します。

add-time:オフセット時間。HH:MM:SS 形式で、HH は 0~23 の範囲の値を取り、MM と SS は 0~59 の範囲の値を取ります。整数に設定する場合は、秒を入力しないでください。整数を設定する場合は、分と秒を入力しないでください。

説明

clock summer-time コマンドは夏時間を設定するのに使用されます。

undo clock summer-time コマンドを使用して、デフォルトの状態を復元します。

他の装置との協調動作を保証し、装置をよりよく監視し、維持するために、装置のシステム時間が正確であることを確認してください。

このコマンドを設定すると、アプライアンスは現在のシステム時間を自動的に再計算し、計算されたシステム時間は **display clock** コマンドで確認できます。

すべてのネットワークデバイスの夏時間を現地の夏時間に合わせます。

例

#夏時間 PDT を設定すると、8 月 1 日の 06:00:00 で始まり、9 月 1 日の 06:00:00 で終わります。これは、現在のデバイスの標準時より 1 時間長くなります。

<AC> system-view

[AC] clock summer-time PDT 6 08/01 6 09/01 1

関連コマンド

- **clock datetime**

- **clock timezone**
- **display clock**

1.1.4 clock timezone

Syntax

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

デフォルト

システムのタイムゾーンは、デバイスが UTC であるゼロタイムゾーンです。

View

System view

定義済みユーザロール

network-admin

パラメータ

zone-name:タイムゾーン名。1~32 文字の文字列で、大文字と小文字が区別されます。

add:指定した時刻を UTC 時刻に追加します。

minus:UTC 時刻から指定した時刻を減算します。

zone-offset:UTC からの時間差。HH:MM:SS 形式。HH は 0~23 の範囲で、MM および SS は 0~59 の範囲で値を取得します。整数に設定する場合は、秒を入力しないでください。整数を設定する場合は、分と秒を入力しないでください。

説明

clock timezone コマンドを使用して、システムのタイムゾーンを設定します。

undo clock timezone コマンドを使用して、デフォルトの状態を復元します。

他の装置との協調動作を保証し、装置をよりよく監視し、維持するために、装置のシステム時間が正確であることを確認してください。

このコマンドを設定すると、アプライアンスは現在のシステム時間を自動的に再計算し、計算されたシステム時間は display clock コマンドで確認できます。

すべてのネットワークデバイスのタイムゾーンと地域のタイムゾーンを一致させてください。

例

#ローカルタイムゾーン名を Z 5 に設定します。

<AC> system-view

[AC] clock timezone Z5 add 5

関連コマンド

- clock datetime
- clock summer-time
- display clock

1.1.5 command

Syntax

command *id command*

undo command *id*

デフォルト

設定なし

View

Job view

定義済みユーザロール

network-admin

パラメータ

id:0~4294967295 の範囲のコマンド番号。この番号はジョブにおける命令の実行順序を表し、番号の小さい命令が優先的に実行される。

command:ジョブに割り当てられたコマンド。

説明

command コマンドは、ジョブにコマンドを割り当てるために使用します。

undo command コマンドジョブに割り当てられたコマンドをキャンセルするために使用します。

command コマンドを複数回入力すると、現在のジョブに複数のコマンドを割り当てることができます。コマンドは番号で一意に区別されます。新しく割り当てられたコマンドの番号が割り当てられたコマンドの番号と同じ場合、新しく割り当てられたコマンドは割り当てられたコマンドを上書きします。

command で割り当てられるコマンドラインは、telnet、ftp、ssh 2、monitor process を除くデバイスで正常に実行されるコマンドラインである必要があります。設定が正しいことはユーザによって確認されます、そうでない場合、コマンドラインは自動的に実行されません。

割り当てが必要なコマンド(A とします)が User View 内のコマンドである場合は、**command** コマンドを使用して直接割り当てることができます。割り当てが必要なコマンド(A とします)が非 User View のコマンドである場合、A を割り当てる前に、A と同じビューに入るコマンド(小さい id 値を指定します。)を割り当てる必要があります。

定期的にタスクを実行する場合、デバイスはユーザと情報をやり取りしません。ユーザによる対話形式の確認が必要な場合は、 「Y」 または「はい」が自動的に入力されます。ユーザが対話的に文字情報を入力する必要がある場合は、デフォルト文字列が自動的に入力され、デフォルト文字列がない場合は空の文字列が自動的に入力されます。

例

#設定ファイル startup.cfg を TFTP サーバ 192.168.100.11 にバックアップするために、backupconfig という名前のジョブにコマンドを割り当てます。

<AC> system-view

[AC] scheduler job backupconfig

[AC-job-backupconfig] command 2 tftp 192.168.100.11 put flash:/startup.cfg backup.cfg

#Job (名前を shutdownGE とします。)にコマンドを割り当てて、インタフェース GigabitEthernet1/0/1 をシャットダウンします。

<AC> system-view

[AC] scheduler job shutdownGE

[AC-job-shutdownGE] command 1 system-view

[AC-job-shutdownGE] command 2 interface gigabitethernet 1/0/1

[AC-job-shutdownGE] command 3 shutdown

関連コマンド

- **scheduler job**

1.1.6 copyright-info enable

Syntax

copyright-info enable

undo copyright-info enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

copyright-info enable コマンドは、著作権情報の表示を有効にします。

undo copyright-info enable コマンドは、著作権情報の表示を無効にします。

例

#著作権情報表示機能を有効にする。

<AC> system-view

[AC] copyright-info enable

1.1.7 diag boot-info display

Syntax

diag boot-info display

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

diag boot-info display コマンドは装置の再起動履歴を表示します。

AC の再起動履歴は、直近で最大 10 件まで表示されます。

例

AC の再起動履歴を表示します。

<AC> diag boot-info display

```
Slot 1:

**************************************************************************
*
PowerOn BootTimes   : 55
Watchdog BootTimes  : 1
Software BootTimes  : 253
Hardware BootTimes  : 0
MotherBoard BootTimes: 0
Backup BootTimes    : 0
CpuS3 BootTimes     : 0
HighTmpr BootTimes  : 0
Slot1Out BootTimes  : 0
Slot2Out BootTimes  : 0
Slot3Out BootTimes  : 0
Hdd1Out BootTimes   : 0
Hdd2Out BootTimes   : 0
```

```
Current Boot Type   : Poweron-boot
Current Running Time: 186000(s)
Running Time        : 2(d)3(h)
*** Boot History(Startup Time and Reason) ***
2015-01-01 00:10:16(GMT+0) Power on
2015-01-01 00:03:24(GMT+0) Power on
2015-01-01 02:34:06(GMT+0) Power on
2015-01-01 00:03:24(GMT+0) Power on
2015-01-01 00:03:18(GMT+0) Power on
2024-01-11 01:44:12(GMT+0) Cloud-cluster merge soft reboot
2024-01-11 01:35:13(GMT+0) Slave switch soft reboot
2024-01-11 00:50:31(GMT+0) User soft reboot
2024-01-09 05:59:33(GMT+0) User soft reboot
2024-01-09 05:29:58(GMT+0) User soft reboot
```

表 1-1 コマンド出力

フィールド	説明
PowerOn BootTimes	Power onが原因で再起動した合計回数です。
Watchdog BootTimes	Watchdog rebootが原因で再起動した合計回数です。
Software BootTimes	soft rebootが原因で再起動した合計回数です。
Hardware BootTimes	Hard rebootが原因で再起動した合計回数です。
MotherBoard BootTimes	Master slotの合計再起動回数です。
Backup BootTimes	Standby slotの合計再起動回数です。
Slot*Out BootTimes	Stanby slotが外れた合計回数です。
Current Boot Type	現在のBootタイプ。 • Unknown • Poweron-boot • Software-boot • Watchdog-boot • Hardware-boot • MotherBoard-boot • ExtendWatchdog-boot • Backup-boot • ExtendedModuleRemoved-boot
Current Running Time	直近のBootの動作時間です。
Running Time	合計の動作時間です。

フィールド	説明
Boot History	下記が表示されます。 原因： ● Power on ● Hard reboot ● Watchdog reboot ● User soft reboot ● Kernel exception soft reboot ● Kernel deadloop soft reboot ● DevHandShake soft reboot ● Lic overTime soft reboot ● Slave switch soft reboot ● Cloud-cluster merge soft reboot ● Auto update soft reboot ● Memory-exhausted reboot ● -Crypto self-test failed reboot サブカテゴリ： ● Reset by admin ● Image was downloaded successfully ● Stayed in idle state for a long time ● WTU reboot because of offline WT ● AP reset from Cloud ● Anomaly detected ● Inconsistent BSS states on AC and AP ● Inconsistent BSS states on AP and in drive ● Inconsistent radio states on AC and AP ● Inconsistent radio modes on AC and AP ● Inconsistent radio rates on AC and AP ● Inconsistent radio channels on AC and AP ● Inconsistent radio bandwidth on AC and AP ● Inconsistent radio interface states on AC and AP ● Inconsistent radio states on AP and in drive ● Inconsistent radio modes on AP and in drive ● Inconsistent radio channels on AP and in drive ● Inconsistent radio bandwidth on AP and in drive

フィールド	説明
	• Anchor AC detected another anchor AC with smaller MAC address and switched its role to AP • Anchor AC received a discovery response and switched its role to AP • Anchor AP failed to detect other anchor ACs or ACs and switched its role to AC • Anchor AC detected another anchor AC with higher priority and switched its role to AP • Configure the anchor device as an AC • Configure the anchor device as an AP • Manually configure the AP to act as a fit AP • Manually configure the AP to act as a fat AP • Manually configure the inside AP to act as a fat AP • Local AC image download • Device role changed from common to local • Device role changed from local to common • Device role changed from common to central • Device role changed from central to common • WT version changed • Cannot process subslot insert event • Cannot send subslot insert event to next step for processing

1.1.8 display clock

Syntax

display clock

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display clock コマンドは、システムの現在の時刻、日付、ローカルタイムゾーン、夏時間設定を表示します。

例

#ローカルタイムゾーンが設定されていない場合は、システムの現在の日付と時刻が表示されます。

<AC> display clock

```
10:09:00 UTC Fri 03/16/2019
```

#ローカルタイムゾーン Z 5 を設定すると、システムの現在の日付と時刻が表示されます。

<AC> display clock

```
15:10:00 Z 5 Fri 03/16/2019
Time Zone :Z 5 add 05:00:00
```

#ローカルタイムゾーン Z 5 および夏時間 PDT が設定されると、システムの現在の日付と時刻が表示されます。

<AC> display clock

```
15:11:00 Z 5 Fri 03/16/2019
Time Zone :Z 5 add 05:00:00
Summer Time :PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

関連コマンド

- **clock datetime**
- **clock timezone**
- **clock summer-time**

1.1.9 display diagnostic-information

Syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename*]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

hardware:ハードウェアに関する診断情報を収集します。

infrastructure:ベースモジュールの診断情報を収集します。

l2:レイヤ 2 特性に関する診断情報を収集する。

l3:レイヤ 3 の特性に関する診断情報を収集する。

service:上位層のビジネスモジュールに関する診断情報を収集します。

key-info:重要な診断情報を収集します。機器の異常や稼働時間が長くなると診断情報が多く発生する可能性があるが、このキーワードを用いることで、重要な診断情報を収集することができ、診断情報の収集時間を短縮することができる。このパラメータを指定しない場合は、現在のすべての診断情報が収集されます。

filename:収集した診断情報を指定したファイルに保存します。filename はファイル名を示し、サフィックスは「.tar.gz」である必要があります。このパラメータが指定されていない場合、ユーザは指定されたファイルに診断情報を保存するか、または診断情報を直接表示するかを選択できます。

説明

display diagnostic-information コマンドを使用して、診断情報を収集します。日常的なメンテナンスやシステム障害の発生時に、問題の特定を容易にするために、各モジュールの診断情報を確認する必要があります。各機能モジュールはそれぞれ実行情報を持っているので、一般にユーザは **display** コマンドを 1 つずつ実行する必要がある。一度に追加情報を収集するために、**display diagnostic-information** コマンドを任意のビューで実行して、複数のモジュールの診断情報を収集できます。

このコマンドを使用すると、指定した診断情報を直接表示したり、診断情報を指定したファイルに直接保存したりできます。診断情報が多いため、このファイルは自動的に圧縮されて保存され、ファイル名には「.tar.gz」という接尾辞が付きます。デバイスでファイルの内容を表示するには、次の手順に従います。

1) tar extract コマンドを使用して、XXXX.tar.gz ファイルを XXXX.gz ファイルにアンパックします。
2) gunzip コマンドを使用して、XXXX.gz ファイルを XXXX ファイルにアンパックします。
3) more コマンドを使用して、XXXX ファイルの内容を表示します。

診断ファイルの収集が途中で中止された場合、gunzip コマンドでは正常に解凍されないことがありますが、診断ファイルに生成された診断情報が含まれている場合は、診断ファイルを PC に転送し、Linux システムの gunzip **-c** コマンドを使用して解凍して表示できます。

filename パラメータを指定せずに **display diagnostic-information** コマンドを実行すると、診断情報を表示するかファイルに保存するかを選択するように求められます。ユーザが診断情報を保存することを選択し、システムがユーザにファイル名を入力するように要求した場合、現在の診断情報は自動的に新しいファイルに保存され、既存のファイルと名前が重複して既存のファイルが上書きされないように、デバイス名と現在のシステム時刻を使用してファイルに名前が付けられます。デバイス名に 「/」 、「¥」 、「:」 、「*」 、 「?」 、<」 、 「>、 「|」 、 「」 などの特殊文字は、診断ファイルに名前を付けるときにアンダースコア 「_」 に変換されます。たとえば、デバイスの名前が A/B である場合、デバイスは flash:/diag_A_B_20160101-000438.tar.gz のような文字列を使用して、新しく生成された診断ファイルに名前を付けます。

hardware、infrastructure、l 2、l 3、service の各パラメータが指定されていない場合は、デバイスによって生成されたすべての診断情報が収集されます。

このコマンドは、「|」 、「>」 、および「>>」パラメータをサポートしていません。

このコマンドを実行して診断情報を収集するときは、収集結果に影響を与えないようにデバイスを構成しないでください。

例

#システムで現在実行されている各機能モジュールの統計情報を収集します。

<AC> display diagnostic-information

```
Save or display diagnostic information (Y=save, N=display)?[Y/N]:n
==============================================
=============== display clock ===============
14:03:55 UTC Thu 01/05/2015
==============================================
=============== display version ===============
```

メッセージ略.....を表示します。

#収集した診断情報をデフォルトの診断ファイルに保存します。

<AC> display diagnostic-information

```
Save or display diagnostic information (Y=save, N=display)?[Y/N]:y
Please input the file name (*.tar.gz) [flash:/diag_Sysname_20160101-
024601.tar.gz]:
Diagnostic information is outputting to flash:/diag_Sysname_20160101-
024601.tar.gz.
Please wait ...
Save successfully.
```

「Please input the file name」の案内で、そのままお車にお戻りください。

#収集した診断情報をファイル test.tar.gz に保存します。

<AC> display diagnostic-information test.tar.gz

```
Diagnostic information is outputting to flash:/test.tar.gz.
Please wait ...
Save successfully.
```

関連コマンド

- **gunzip (基本機能/ファイルシステム管理)**
- **more (基本機能/ファイルシステム管理)**
- **tar extract (基本機能/ファイルシステム管理)**

1.1.10 display scheduler job

Syntax

display scheduler job [*job-name*]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

job-name:ジョブの名前。1~47 文字の文字列で、大文字と小文字が区別されます。このパラメータを指定しない場合は、すべてのジョブの構成情報が表示されます。

説明

display scheduler job コマンドは、スケジュールされた実行タスクのジョブの構成情報を表示します。

例

#スケジュールされたすべてのタスクのジョブの構成情報を表示します。

<AC> display scheduler job

```
Job name:saveconfig
copy startup.cfg backup.cfg

Job name:backupconfig

Job name:creat-VLAN100
system-view
vlan 100
```

上記の情報は、デバイスに現在設定されている 3 つのジョブがあり、それぞれのジョブの名前と、ジョブに割り当てられたコマンド(ジョブにコマンドが割り当てられていない場合は、ジョブの名前のみが表示されます。)が空白行で区切られて表示されていることを示しています。

1.1.11 display scheduler logfile

Syntax

display scheduler logfile

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display scheduler logfile コマンドは、Schedule ログファイルに関する情報を表示します。

例

#Schedule ログファイルに関する情報を表示します。

<AC> display scheduler logfile

```
Logfile Size:1902 Bytes.

Job name:shutdown
Schedule name:shutdown
Execution time:Tue Dec 27 10:44:42 2019
Completion time :Tue Dec 27 10:44:47 2019
--------------------------------- Job output ---------------------------------
```

<AC> system-view

```
System View:return to User View with Ctrl+Z.
```

[AC] interface rang gigabitethernet 1/0/1 to gigabitethernet 1/0/3

[AC-if-range] shutdown

表 1-2 display scheduler logfile コマンドの表示情報の説明

フィールド	説明
Logfile Size	Scheduleバイト単位のログファイルのサイズ
Job name	ジョブの名前
Schedule name	Scheduleの名前
Execution time	ジョブの実行が開始された時刻
Completion time	ジョブ実行終了時刻(スケジュールされていないジョブまたはコマンドが割り当てられていないジョブでは、この情報は表示されません。)
Job output	ジョブでのコマンド実行時の出力情報

関連コマンド

- **reset scheduler logfile**

1.1.12 display scheduler reboot

Syntax

display scheduler reboot

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display scheduler reboot コマンドを使用して、スケジュールされた再起動機能の設定を表示します。

例

#タイムリスタート機能の設定を表示します。

<AC> display scheduler reboot

```
System will reboot at 16:32:00 05/23/2019 (in 1 hours and 39 minutes).
```

関連コマンド

- **scheduler reboot at**
- **scheduler reboot delay**

1.1.13 display scheduler schedule

Syntax

display scheduler schedule [*schedule-name*]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

schedule-name:Schedule の名前。1~47 文字の文字列で、大文字と小文字が区別されます。このパラメータを指定しない場合は、すべての Schedule の情報が表示されます。

説明

display scheduler schedule コマンドは、スケジュールされた実行タスクに関する情報を表示します。

例

#スケジュールされたすべてのタスクの情報を表示します。

<AC> display scheduler schedule

Schedule name:shutdown

Schedule type:Run once after 0 hours 2 minutes

Start time:Tue Dec 27 10:44:42 2019

Last execution time:Tue Dec 27 10:44:42 2019

Last completion time :Tue Dec 27 10:44:47 2019

Execution counts:1

Job nameLast execution status

shutdownSuccessful

表 1-3 display scheduler schedule コマンドの表示情報の説明

フィールド	説明
Schedule name	Scheduleの名前
Schedule type	Scheduleの実行時間を設定します。Scheduleに実行時間が設定されていない場合、この情報は表示されません。
Start time	Schedule最初に実行を開始した時刻。Scheduleに実行時間が設定されていない場合、この情報は表示されません。
Last execution time	Schedule最後に実行が開始された時刻 • Schedule に実行時間が設定されていない場合、この情報は表示されません。 • まだ実行されていない場合は、Yet to be executed と表示されます。
Last completion time	Schedule最後の実行が完了した時刻。Scheduleに実行時間が設定されていない場合、この情報は表示されません。
Execution counts	Scheduleが実行された回数。Scheduleがまだ実行されていない場合、この情報は表示されません。
Job name	Scheduleで関連付けられているジョブの名前

フィールド	説明
Last execution status	ジョブが最後に実行されたときの状態(ジョブに割り当てられたコマンドが実行されたかどうか、および実行結果を確認するには、display scheduler logfileコマンドを使用します。) • Successful:実行が成功したことを示します。 • Failed:実行に失敗したことを示します。 • Waiting:実行待ちであることを示します。 • In process:実行中であることを示します。 • -NA-:実行時刻になっていないことを示します。

1.1.14 header

Syntax

header { **incoming** | **legal** | **login** | **motd** | **shell** } *text*

undo header { **incoming** | **legal** | **login** | **motd** | **shell** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

incoming:Modem ログインユーザのログイン User View へのようこそを設定します。認証が必要な場合は、認証に合格するとウェルカムメッセージが出力されます。

legal 認証ユーザ名およびパスワードを入力する前に出力されるログインエンドポイントインタフェースの前の認証情報を設定して下さい。

login:ログイン認証のためのウェルカムメッセージを設定します。

motd:端末インタフェースにログインするためのウェルカムメッセージを設定します。

shell:Modem 以外のログインユーザが User View にログインする場合の開始情報を設定します。

text:開始メッセージの内容。コンテンツの入力は、1 行または複数行の両方をサポートしています。具体的な入力規則は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*1 章 装置管理*”を参照してください。

説明

header コマンドを使用して、開始メッセージを設定します。

undo header コマンドを使用して設定を解除します。

例

#設定 legal ようこそ。

<AC> system-view

[AC] header legal

```
Please input banner content、and quit with the character '%'.
Welcome to use the legal banner%
```

1.1.15 job

Syntax

job *job-name*

undo job *job-name*

デフォルト

Schedule にジョブが割り当てられていません。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

job-name:ジョブの名前。1~47 文字の文字列で、大文字と小文字が区別されます。

説明

job コマンドは、Schedule にジョブを割り当てるために使用します。

undo job コマンドは、Schedule からジョブを削除するために使用します。

このコマンドを複数回実行すると、Schedule に複数のジョブを割り当てることができます。複数のジョブは、Schedule で指定された時刻に、順序なしで同時に実行されます。

割り当てられるジョブは、デバイス上ですでに作成されているジョブである必要があります。それ以外のジョブは割り当てられません。ジョブは、scheduler job コマンドを使用して作成できます。

例

#Schedule に save-job という名前のジョブを割り当てます。

<AC> system-view
[AC] scheduler schedule saveconfig
[AC-schedule-saveconfig] job save-job

関連コマンド

- **scheduler job**
- **scheduler schedule**

1.1.16 locator blink

🕮 **メモ：**

locator blink コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

locator blink *blink-time* [**ap** *ap-name*]

locator blink stop [**ap** *ap-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

blink-time: LED を点滅させる時間を秒単位で指定します。設定範囲は 5 から 120 秒です。

stop: LED の点滅を停止します。

ap *ap-name*: AP 名を指定します。設定範囲は 1～64 文字で大文字、小文字を区別します。文字列には、英字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含めることができます。

🕮 **メモ：**

- **ap** *ap-name* パラメータは、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。
- **ap** *ap-name* パラメータを省略して実行した場合、コマンドを実行した装置の SYS LED が点滅します。
- **ap** *ap-name* パラメータを指定して実行した場合、指定した AP の電源 LED が点滅します。

説明

locator blink *blink-time* コマンドは、指定した装置の LED を *blink-time* で指定した時間緑→赤の順に点滅させます。**locator blink stop** コマンドを実行すると、**locator blink** *blink-time* コマンドによる LED の点滅を停止します。

本機能は装置の位置を特定する際に役立ちます。

例

点滅時間を 30 秒に指定して SYS LED の点滅を開始します。

<AP> locator blink 30

SYS LED の点滅を停止します。

<AP> locator blink stop

1.1.17 reboot

Syntax

reboot [**slot** *slot-number*] [**force**]

View

User View

定義済みユーザロール

network-admin

パラメータ

slot slot-number: メンバ ID によってクラウドクラスタのメンバ装置を指定します。このオプションが指定されない場合、クラウドクラスタではすべての装置を再起動します。

force:強制再起動:

- このパラメータを指定しない場合、デバイスを再起動すると、システムは保護性検査(スタートアップ・ファイルが存在するかどうか、ディスクが書き込まれているかどうかなど)を行い、検査に合格しなければ処理を終了し、デバイスを再起動しない。
- このパラメータを指定すると、システムはチェックを行わずに再起動を実行します。

説明

reboot コマンドを使用してデバイスを再起動します。

 注意

- 再起動すると業務が中断されることがあります。このコマンドは注意して使用してください。
- デバイスに障害が発生した場合、または force キーワードを指定しないで再起動コマンドを実行しても再起動を正しく実行できない場合にのみ、force キーワードを使用してください。force キーワードを指定した再起動コマンドは、データ保護を実行しないため、ファイルシステムが破損する可能性があります。

メインスタートアップソフトウェアイメージが破損または欠落している場合は、**reboot** コマンドを実行する前に、メインスタートアップソフトウェアイメージのセットを再設定する必要があります。

データ保護のため、デバイスがファイル操作を実行している間にデバイスを再起動しても、デバイスは再起動しません。

例

#デバイスを再起動し、構成ファイルを保存します。

```
<AC> reboot
Start to check configuration with next startup configuration file, please wait ..... DONE!
Current configuration will be lost after the reboot、save current configuration?[Y/N]:y
Please input the file name (*.cfg) [flash:/startup.cfg]
(To leave the existing filename unchanged、press the enter key):
flash:/startup.cfg exists, overwrite?[Y/N]:y
Validating file.Please wait ...
Configuration is saved to device successfully.
This command will reboot the device.Continue?[Y/N]:y
Now rebooting, please wait ...
```

#デバイスを強制的に再起動します。

```
<AC> reboot force
A forced reboot might cause the storage medium to be corrupted.Continue?[Y/N]:y
Now rebooting, please wait ...
```

関連コマンド

- **display system stable state**

1.1.18 reset scheduler logfile

Syntax

reset scheduler logfile

View

User View

定義済みユーザロール

network-admin

説明

reset scheduler logfile コマンドは、Schedule ログファイルに関する情報をクリアするために使用します。

例

#Schedule ログファイルに関する情報をクリアします。

<AC> reset scheduler logfile

関連コマンド

- **display scheduler logfile**

1.1.19 restore factory default

Syntax

restore factory-default

View

User view

定義済みユーザロール

network-admin

説明

restore factory-default コマンドは装置を工場出荷時のデフォルト状態に復元します。

注意：

このコマンドは注意して使用してください。デバイスを別の用途で使用する場合、または他の方法を使用してデバイスのトラブルシューティングを行うことができない場合のみ、このコマンドを使用してください。

例

装置を工場出荷時のデフォルト状態に復元します。

<AC> restore factory-default

```
This command will restore the system to the factory default configuration and
clear the operation data, and forcibly reboot the system. Continue [Y/N]:y
Restoring the factory default configuration. This process might take a few
minutes. Please wait....Done.
The system is rebooting...
```

1.1.20 scheduler job

Syntax

scheduler job *job-name*

undo scheduler job *job-name*

デフォルト

ジョブは存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

job-name:ジョブの名前。1~47 文字の文字列で、大文字と小文字が区別されます。

説明

scheduler job コマンドを使用してジョブを作成し、Job view に移動します。指定したジョブがすでに存在する場合は、 Job view に直接移動します。

undo scheduler job コマンドは、作成されたジョブを削除するために使用します。

ジョブは複数の Schedule によって参照できます。Job view の下のユーザは、**command** コマンドを使用してジョブにコマンドを割り当てることができます。

例

#backupconfig という名前のジョブを作成し、Job view に移動します。

<AC> system-view
[AC] scheduler job backupconfig
[AC-job-backupconfig]

関連コマンド

- **command**
- **scheduler schedule**

1.1.21 scheduler logfile size

Syntax

scheduler logfile size *value*

デフォルト

Schedule ログファイルのサイズは 16 KB です。

View

System view

定義済みユーザロール

network-admin

パラメータ

value:Schedule ログファイルのサイズは、16~1024 KB の範囲で指定できます。

説明

scheduler logfile size コマンドは、Schedule ログファイルのサイズを設定します。

Schedule ログファイルは、ジョブの次のコマンドラインの実行結果を記録します。ファイルのサイズがユーザ設定値を超えると、古いレコードが削除され、新しいレコードが記録されます。ログファイルのサイズを超えるログ情報を記録する場合、ログの超過部分は記録されません。

例

#設定 Schedule ログファイルのサイズは 32 KB です。

<AC> system-view

[AC] scheduler logfile size 32

関連コマンド

- **display scheduler logfile**

1.1.22 scheduler reboot at

Syntax

scheduler reboot at *time* [*date*]

undo scheduler reboot

デフォルト

デバイスの再起動の日時は設定されていません。

View

User View

定義済みユーザロール

network-admin

パラメータ

time:HH:MM の形式でデバイスが再起動された時刻。HH は時間、0~23 の範囲、MM は分、0~59 の範囲です。

date:デバイスが再起動した日付。MM/DD/YYYY (月/日/年)または YYYY/MM/DD (年/月/日)の形式になります。

- YYYY の範囲は 2000~2035 です。
- MM の範囲は 1~12 です。
- DD の範囲は、特定の月に関連しています。

説明

scheduler reboot at コマンドを使用して、デバイスの再起動の日時を設定します。

undo scheduler reboot コマンドは、スケジュールされた再起動設定をキャンセルするために使用します。

注意

このコマンドを使用すると、デバイスが将来のある時点で再起動され、業務が中断される可能性があります。注意して使用してください。

---

date パラメータが指定されていない場合は、次のようになります。

- 構成された時点が現在の時刻より後の場合、デバイスはその日のその時点で再起動されます。
- 構成された時点が現在の時刻より前である場合、デバイスは翌日のその時点で再起動します。

scheduler reboot at、scheduler reboot delay コマンドを複数回設定すると、最後に実行されたコマンドが有効になります。

デバイスの再起動の準備中にユーザがファイル操作を実行している場合は、セキュリティ上の理由から再起動は実行されません。

例

#システムの現在の時刻が 2019 年 6 月 6 日 11:43 であると仮定すると、デバイスはその日の正午 12:00 に再起動します。

<AC> scheduler reboot at 12:00

```
Reboot system at 12:00:00 06/06/2019 (in 0 hours and 16 minutes).Confirm?[Y/N]:
```

関連コマンド

- **scheduler reboot delay**

1.1.23 scheduler reboot delay

Syntax

scheduler reboot delay *time*

undo scheduler reboot

デフォルト

デバイスの再起動の遅延時間は設定されていません。

View

User View

定義済みユーザロール

network-admin

パラメータ

time:HH:MM (時間:分)または MM (分)形式のデバイス再起動の待機時間。

- HH:MM フォーマットの場合、MM の値は 0~59 の範囲で、HH:MM の最大長は 6 文字です。
- MM 形式の場合、最大長は 6 文字です。

説明

デバイスを再起動する遅延時間を設定するには、**scheduler reboot delay** コマンドを使用します。

undo scheduler reboot コマンドは、スケジュールされた再起動設定をキャンセルするために使用します。

注意

このコマンドを使用すると、デバイスが将来のある時点で再起動され、業務が中断される可能性があります。注意して使用してください。

scheduler reboot at、**scheduler reboot delay** コマンドを複数回設定すると、最後に実行されたコマンドが有効になります。

デバイスの再起動の準備中にユーザがファイル操作を実行している場合は、セキュリティ上の理由から再起動は実行されません。

例

#システムの現在の時刻が 2019 年 6 月 6 日 11:48 で、88 分後にデバイスを再起動するように設定されているとします。

<AC> scheduler reboot delay 88

```
Reboot system at 13:16 06/06/2019 (in 1 hours and 28 minutes).Confirm?[Y/N]:
```

関連コマンド

- **scheduler reboot at**

1.1.24 scheduler schedule

Syntax

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

デフォルト

Schedule は存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

schedule-name:Schedule の名前。1~47 文字の文字列で、大文字と小文字が区別されます。

説明

scheduler schedule コマンドを使用して Schedule を作成し、対応する Schedule view に移動します。指定した Schedule がすでに存在する場合は、Schedule view に直接移動します。

undo scheduler schedule コマンドは、指定された Schedule を削除するために使用します。

scheduler schedule コマンドを使用して、デバイスが指定された時間に指定されたコマンドを実行するようにスケジュールされたタスクを設定します。

構成手順は次のとおりです。

1) scheduler job コマンドを使用してジョブを作成します。
2) Job view で、command コマンドを使用して実行する必要があるコマンドを設定します。
3) scheduler schedule コマンドを使用して Schedule を作成します。
4) Schedule view で、ジョブコマンドを使用して Schedule にジョブを割り当てます。1 つの Schedule に複数のジョブを割り当てることができますが、作成されたジョブである必要があります。そうでない場合、割り当ては失敗します。
5) Schedule view で、user-role コマンドを使用して Schedule のユーザロールを設定します。1 つの Schedule に最大 64 個のロールを割り当てることができます。
6) Schedule view で、time at、time once、または time repeating コマンドを使用して、タスクの実行時間を設定します。Schedule で設定できる実行時間は 1 つだけです。

例

#saveconfig という名前の Schedule を作成します。

<AC> system-view

[AC] scheduler schedule saveconfig

関連コマンド

- **job**
- **time at**
- **time once**

1.1.25 sysname

Syntax

sysname *sysname*

undo sysname

デフォルト

QX-W2300AC シリーズ

View

System view

定義済みユーザロール

network-admin

パラメータ

sysname:デバイス名。1~64 文字の文字列です。

説明

sysname コマンドは、デバイスの名前を設定します。

undo sysname を使用して、デフォルトの状態を復元します。

デバイス名はコマンドラインインタフェースのプロンプトに対応します。たとえば、デバイス名が Sysname の場合、User View のプロンプトは<AC>になります。

例

#設定デバイス名は MyDevice です。

<AC> system-view

[AC] sysname MyDevice

[MyDevice]

1.1.26 time at

Syntax

time at *time date*

undo time

デフォルト

Schedule の実行時間が設定されていません。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

time:Schedule の実行時間を HH:MM (時間:分)形式で指定します。HH の範囲は 0~23、MM の範囲は 0~59 です。

date:Schedule が MM/DD/YYYY (月/日/年)または YYYY/MM/DD (年/月/日)の形式で実行された日付。

- YYYY の範囲は 2000~2035 です。
- MM の範囲は 1~12 です。
- DD の範囲は、特定の月に関連しています。

説明

time at コマンドは、指定した時刻に Schedule を実行するように設定するために使用します。

undo time コマンドは、Schedule の時間設定をキャンセルするために使用します。

構成のポイントインタイムは、システムの現在のポイントインタイムよりも後にする必要があります。それ以外の場合、構成は失敗します。

1 つの Schedule に設定できる実行時間は 1 つだけです。したがって、同じ Schedule view で **time at**、**time once**、または **time repeating** コマンドを複数回実行すると、最後に実行されたコマンドが有効になります。

例

#設定 2019 年 5 月 11 日 1:01 saveconfig という名前の Schedule を実行します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time at 1:1 2019/05/11

関連コマンド

- **scheduler schedule**
- **time once**
- **time repeating**

1.1.27 time once

Syntax

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

time once delay *time*

undo time

デフォルト

Schedule の実行時間が設定されていません。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*:Schedule の実行時間を HH:MM (時間:分)形式で指定します。HH の範囲は 0~23、MM の範囲は 0~59 です。

month-date *month-day*:Schedule が実行される月の日。month-day は日付を表し、1~31 の値を取ります。月が存在しない日付を指定した場合、実際に有効になるのは次の月の日付です。たとえば、2 月に 30 がない場合、実際に有効になるのは 3 月の 30 です。

week-day week-day& <1-7>:Schedule が実行される曜日。week-day& <1-7>は曜日または曜日の組み合わせを表し、week-day は Mon、Tue、Wed、Thu、Fri、Sat、Sun の値を取り、&<1-7>は前のパラメータが最大 7 回入力できることを示します。複数日構成の場合、文字列はスペースで区切られます。

delay *time*:Schedule が実行を遅らせる時間を指定します。形式は HH:MM (時間:分)または MM (分)です。

- HH:MM フォーマットの場合、MM の値は 0~59 の範囲で、HH:MM の最大長は 6 文字です。
- MM 形式の場合、最大長は 6 文字です。

説明

time once コマンドは、Schedule の実行時間を設定するために使用します。

undo time コマンドは、Schedule の時間設定をキャンセルするために使用します。

このコマンドが設定されると、Schedule は設定された時点に到達した時点で実行され、その日/月/週の時点が経過すると、次の日/月/週に延期されます。実行後、次にその時点に到達したとき Schedule は実行されません。

1 つの Schedule に設定できる実行時間は 1 つだけです。したがって、同じ Schedule view で **time at**、**time once**、または **time repeating** コマンドを複数回実行すると、最後に実行されたコマンドが有効になります。

例

#この日の 15 時に saveconfig という名前の Schedule を実行します。

<AC> system-view
[AC] scheduler schedule saveconfig
[AC-schedule-saveconfig] time once at 15:00

#最後に到着した 15 番の 15 時に saveconfig という名前の Schedule を実行します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time once at 15:00 month-date 15

#最後の月曜日と金曜日の 12 時ちょうどに、saveconfig という名前の Schedule が実行されます。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time once at 12:00 week-day mon fri

#10 分遅れて saveconfig という名前の Schedule が実行されます。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time once delay 10

関連コマンド

- **scheduler schedule**
- **time at**
- **time repeating**

1.1.28 time repeating

Syntax

time repeating [at *time [date]***] interval** *interval*

time repeating at *time* **[month-date [***month-day* **|last]|week-day** *week-day& <1-7>]*

undo time

デフォルト

Schedule を繰り返し実行する時間は設定されていません。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*:HH:MM (時間:分)形式で繰り返し実行される時間を示します。HH の範囲は 0~23、MM の範囲は 0~59 です。このパラメータを指定しない場合は、これから開始することを意味します。

date:Schedule の繰り返しの開始日を MM/DD/YYYY (月/日/年)または YYYY/MM/DD (年/月/日)の形式で指定します。このパラメータが指定されていない場合は、time の時点に将来最初に到達する日付を表します。

- YYYY の範囲は 2000~2035 です。
- MM の範囲は 1~12 です。
- DD の範囲は、特定の月に関連しています。

interval *interval*:繰り返し実行の間隔を指定します。形式は HH:MM (時間:分)または MM (分)です。

- HH:MM フォーマットの場合、MM の値の範囲は 0~59 で、最大長は 6 文字です。

- MM フォーマットの場合、最小値は 1、最大長は 6 文字です。

month-date *[month-day |last]*:各月の 1 日を表します。ここで、month-day は日付を表し、1~31 の値を取ります。月が存在しない日付を指定した場合、実際に有効になるのは次の月の日付です。たとえば、2 月に 30 がない場合、実際に有効になるのは 3 月の 30 です。last は毎月の最終日を表します。

week-day week-day& <1-7>:曜日を示す。week-day& <1-7>は曜日または曜日の組み合わせを表し、week-day は Mon、Tue、Wed、Thu、Fri、Sat、Sun の値を取り、&<1-7>は前のパラメータが最大 7 回入力できることを示します。複数日構成の場合、文字列はスペースで区切られます。

説明

time repeating コマンドは、Schedule を繰り返し実行する時間を設定します。

undo time コマンドは、Schedule の時間設定をキャンセルするために使用します。

time repeating [at time [date]] interval interval は、Schedule が指定された時刻から定期的に実行されることを示します。

time repeating at time [month-date [month-day |last]|week-day week-day& <1-7>]は、毎月または毎週、Schedule を繰り返すことを意味します。

1 つの Schedule に設定できる実行時間は 1 つだけです。したがって、同じ Schedule view で **time at**、**time once**、または **time repeating** コマンドを複数回実行すると、最後に実行されたコマンドが有効になります。

例

#設定午前 8 時に開始し、1 時間ごとに saveconfig という名前の Schedule を実行します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 8:00 interval 60

#設定これから毎日 12:00 に saveconfig という名前の Schedule を実行します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 12:00

#設定これから毎月 5 日の午前 8 時に saveconfig という名前の Schedule を実行します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 8:00 month-date 5

#設定毎月最終日の 8 時に、saveconfig という名前の Schedule を実行します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 8:00 month-date last

#設定これ以降、毎週金曜日と土曜日の午前 8 時に、saveconfig という名前の Schedule を実行します。

<AC> system-view

[AC] scheduler schedule saveconfig

[AC-schedule-saveconfig] time repeating at 8:00 week-day fri sat

関連コマンド

- **scheduler schedule**
- **time at**
- **time once**

1.1.29 user-role

Syntax

user-role *role-name*

undo user-role *role-name*

デフォルト

Schedule 作成者のユーザロール。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。1～63 文字の大文字小文字を区別する文字列です。ユーザロールはユーザ定義または事前定義されているものが使用できます。事前定義されたユーザロールには、network-admin、network-operator、level-0 から level-15 があります。

説明

user-role コマンドは、Schedule にユーザロールを割り当てます。

undo user-role コマンドは Schedule からユーザロールを削除します。

Schedule には 1 つ以上のユーザロールが必要です。Schedule 内のコマンドは、その Schedule の 1 つ以上のユーザロールによって許可されている場合に実行できます。ユーザロールに関する詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。

このコマンドを複数回実行することで Schedule に最大 64 個のユーザロールを設定できます。上限に達した場合、追加のユーザロールをスケジュールに割り当てることはできません。

例

#スケジュール test にユーザロール rolename を割り当てます。

<AC> system-view
[AC] scheduler schedule test
[AC-schedule-test] user-role rolename

関連コマンド

scheduler schedule

目次

このセクションのページは **3-x-x** です。

2 章 装置ハードニング 2-1
2.1 装置ハードニングコマンド 2-1
2.1.1 password-recovery enable 2-1

2章 装置ハードニング

2.1 装置ハードニングコマンド

2.1.1 password-recovery enable

Syntax

password-recovery enable

undo password-recovery enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

password-recovery enable コマンドを使用して、パスワード回復機能を有効にします。

undo password-recovery enable コマンドを使用して、パスワード回復機能を無効にします。

パスワード回復機能を設定した後、ユーザーが Console のパスワードを忘れた場合、またはログイン認証に失敗した場合、コマンドラインを使用してデバイスを操作できなくなった場合は、Boot メニューを使用して認証パスワードをクリアしてから、デバイスの使用を再開してください。パスワード回復機能をオフにすると、デバイスはより安全な状態になります。つまり、このような状況が発生した場合、Console ポートを使用してデバイスに対するコマンドライン操作を継続するには、Boot メニューでデバイスを工場出荷時の状態に戻してから操作を継続するしかありません。これにより、不正なユーザーが起動プロファイルを取得することを有効に防止できます。

例

#パスワードの復元を無効にします。

<Sysname> system-view

[Sysname] undo password-recovery enable

```
The command will disable the password recovery function.Continue?[Y/N]:
```

目次

このセクションのページは **3-x-x** です。

3 章 ハードウェアリソース管理 3-1
3.1 ハードウェアリソース管理コマンド 3-1
3.1.1 display cpu-usage 3-1
3.1.2 display cpu-usage history 3-2
3.1.3 display device 3-4
3.1.4 display device manuinfo 3-5
3.1.5 display environment 3-6
3.1.6 display memory 3-7
3.1.7 display memory-threshold 3-9
3.1.8 display transceiver alarm 3-11
3.1.9 display transceiver diagnosis 3-13
3.1.10 display transceiver interface 3-14
3.1.11 display transceiver manuinfo 3-16
3.1.12 memory-threshold 3-17
3.1.13 monitor cpu-usage enable 3-19
3.1.14 monitor cpu-usage interval 3-20
3.1.15 monitor cpu-usage threshold 3-21
3.1.16 shutdown-interval 3-22
3.1.17 temperature-limit 3-23

3章 ハードウェアリソース管理

3.1 ハードウェアリソース管理コマンド

3.1.1 display cpu-usage

Syntax

display cpu-usage [**control-plane** | **data-plane**] [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

control-plane:CPU 使用率に関するコントロールプレーンの統計情報を表示します。このパラメータのサポート状況はデバイスのモデルに依存します。デバイスの実際の状況に基づいてください。

data-plane:CPU 使用率の統計を表示します。このパラメータのサポート状況はデバイスのモデルに依存します。デバイスの実際の状況に基づいてください。

summary:CPU 使用率の統計をリスト表示します。このパラメータを指定しない場合は、CPU 使用率の統計がセクションとして表示されます。

説明

display cpu-usage コマンドは、CPU 使用率の統計を表示するために使用します。

過去 5 秒、1 分、5 分の CPU 使用率の値が「--」と表示された場合は、コマンドラインでデバイスの内部データベースからのデータ取得に失敗した可能性があります。しばらくお待ちください。

例

#現在の CPU 使用率の統計をセグメントとして表示します。

<Sysname> display cpu-usage

```
CPU usage:
1% in last 5 seconds
1% in last 1 minute
1% in last 5 minutes
```

#現在の CPU 使用率の統計を表形式で表示します。

<Sysname> display cpu-usage summary

```
CPULast 5 secLast 1 minLast 5 min
02%2%10%
```

表 3-1 display cpu-usage コマンドの表示情報の説明

フィールド	説明
1% in last 5 seconds	デバイスが起動すると、5秒間のCPUの平均使用率が5秒ごとに計算され、記録されます。このフィールドには、過去5秒間のCPUの平均使用率が表示されます。
Last 5 sec	デバイスが起動すると、5秒間のCPUの平均使用率が5秒ごとに計算され、記録されます。このフィールドには、過去5秒間の統計期間におけるCPUの平均使用率が表示されます。Last 5 secの値が「--」の場合、統計情報はサポートされていません
1% in last 1 minute	デバイスが起動すると、その1分間のCPUの平均使用率が1分間隔で計算され、記録されます。このフィールドには、過去1分間の統計サイクルにおけるCPUの平均使用率が表示されます。
Last 1 min	デバイスが起動すると、その1分間のCPUの平均使用率が1分間隔で計算され、記録されます。このフィールドには、過去1分間の統計サイクルにおけるCPUの平均使用率が表示されます。Last 1 minの値が「--」の場合、統計情報はサポートされていません
1% in last 5 minutes	デバイスが起動すると、その5分間のCPUの平均使用率が5分ごとに計算され、記録されます。このフィールドには、過去5分間の統計期間におけるCPUの平均使用率が表示されます。
Last 5 min	デバイスが起動すると、その5分間のCPUの平均使用率が5分ごとに計算され、記録されます。このフィールドには、過去5分間の統計サイクルにおけるCPUの平均使用率が表示されます。Last 5 minの値が「--」の場合、統計情報はサポートされていません

3.1.2 display cpu-usage history

Syntax

display cpu-usage history [**job** *job-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

job *job-id*:指定したプロセスの CPU 使用率の履歴情報を表示します。*job-id* は 1~2147483647 の範囲でプロセス番号を示します。このパラメータを指定しない場合は、システム全体に関する情報が表示されます。システム全体の CPU 使用率は、すべてのプロセスの CPU 使用率の合計と等しくなります。

説明

display cpu-usage history コマンドは、CPU 使用率の履歴情報をグラフ表示します。

CPU 利用率履歴機能を起動すると、システムは一定時間(**monitor cpu-usage interval** コマンドで設定可能)ごとに CPU の利用率をサンプリングし、サンプリング結果を履歴エリアに保存する。**display cpu-usage history** コマンドを使用すると、最新の 60 個のサンプルポイントの値を表示できます。結果は座標で表示され、次の情報が表示されます。

- 縦軸は利用率を表し、近くに表示する原則を採用している。たとえば、使用率の間隔が 5%の場合、実際の統計値 53%は 55%、実際の統計値 52%は 50%と表示されます。
- 横軸は時間を表し、時間が左になるほど現在の時間に近づきます。
- その時点での利用率を連続した#番目で表し、ある時点で最も高い#番目に対応する縦軸の値がその時点での CPU の利用率となる。

例

#CPU 使用率の履歴をグラフで表示します。

<Sysname> display cpu-usage history

```
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|           #
 10%|          ###  #
  5%|         ########
```

```
------------------------------------------------------------
        10        20        30        40        50        60  (minutes)
               cpu-usage (Slot 1 CPU 0) last 60 minutes (SYSTEM)
```

上記の情報は、最近 60 分間のシステム(「SYSTEM」で表す)の CPU 使用率が、12 分前が約 5%、13 分前が約 10%、14 分前が約 15%、15 分前が約 10%、16、17 分前が約 5%、18 分前が約 10%、19 分前が約 5%、その他の時間が 2%以下であることを示しています。

関連コマンド

- **monitor cpu-usage enable**
- **monitor cpu-usage interval**

3.1.3 display device

Syntax

display device [**flash**] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

flash:Flash の情報を表示します。

verbose:デバイスの詳細を表示します。このパラメータを指定しないと、デバイスの簡単な情報が表示され、ファイアウォールカードの情報は表示されません。

説明

display device コマンドを使用して、デバイスのハードウェア情報を表示します。

flash パラメータを指定しない場合は、デバイスのハードウェア情報が表示されます。

例

#デバイスのハードウェア情報を表示します。

<Sysname> display device

```
Slot No.  Subslot No. Board Type       Status    Max Ports
1         0          WX3510X          Normal     17
1         3          EWPXM1XG03       Normal     10
```

表 3-2 display device コマンドの表示情報の説明

フィールド	説明
Board Type	デバイスのハードウェアタイプ
Status	デバイスの状態: ● Illegalは、デバイスが機能していないことを示します。 ● Normalは、デバイスが正常に機能していることを示します。
Max Ports	デバイスの物理ポート数

3.1.4 display device manuinfo

Syntax

display device manuinfo [**subslot** *subslot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

subslot *subslot-number*:指定したドーターカードの電子タグ情報を表示します。subslot-number は、ドーターカードがあるサブスロットタグを示します。このパラメータを指定しないと、ドーターカードの情報は表示されません。

説明

display device manuinfo コマンドは、デバイスハードウェアの電子タグ情報を表示します。

電子タグ情報は、ハードウェアの名前、製造シリアル番号、MAC アドレス、製造者等の情報を含む、ハードウェアの計測(デバッグ、テスト)中に装置の記憶装置に書き込まれる永久構成データ又はアーカイブ情報等とも呼ばれる。

例

#デバイスハードウェアの電子タグ情報を表示します。

<Sysname> display device manuinfo

...

3.1.5 display environment

Syntax

display environment

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display environment コマンドを使用して温度情報を表示します。

例

温度情報を表示します。

<Sysname >display environment

```
System Temperature information (degree centigrade):
---------------------------------------------------
Slot    Sensor               Temperature  LowerLimit  WarningLimit  AlarmLimit
ShutdownLimit
1     inflow  1     24         0         59          64         80
1     hotspot 1(cpu)64          0          86          89          N/A
1     outflow 1     43         0         100         117        122
```

表 3-3 display environment コマンドの表示情報の説明

フィールド	説明
System Temperature information (degree centigrade)	温度情報（℃）
sensor	温度センサ • **hotspot**—ホットスポットセンサ • **inflow**—吸気口周辺の温度センサ • **outflow**—排気口周辺の温度センサ
Slot	スロット番号
Temperature	現在の温度
Lower	下限しきい値。このフィールドをサポートしていない場合は**NA**と表示します。

フィールド	説明
Warning	ワーニングしきい値。 このフィールドをサポートしていない場合は**NA**と表示します。
Alarm	アラームしきい値。このフィールドをサポートしていない場合は**NA**と表示します。
Shutdown	シャットダウンしきい値。シャットダウンしきい値を超えると、装置は再起動します。このフィールドをサポートしていない場合は**NA**と表示します。 シャットダウンしきい値は**temperature-limit**コマンドで変更できません。

3.1.6 display memory

Syntax

display memory [**summary**]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

summary:メモリ使用量に関する簡単な情報を表示します。このパラメータを指定しない場合は、メモリ使用量の詳細が表示されます。

説明

display memory コマンドを使用して、メモリ使用量を表示します。

表示されたメッセージの 1 行に、すべてのパラメータの値が「--」と表示されている場合は、コマンドラインでデバイスの内部データベースからデータを取得できなかった可能性があります。しばらくしてからやり直してください。

例

#デバイスのメモリ使用量の詳細を表示します。

<Sysname> display memory

```
Memory statistics are measured in KB:
           Total      Used      Free    Shared   Buffers    Cached   FreeRatio
Mem:       507980    154896    353084         0       488     54488       69.5%
-/+ Buffers/Cache:     99920    408060
```

```
Swap:          0        0        0
LowMem:     888420    80776   807644       --       --       --      90.9%
HighMem:    904128   564844   339284       --       --       --      37.5%
```

#デバイスのメモリ使用量に関する簡単な情報を表示します。

<Sysname> display memory summary

```
Memory statistics are measured in KB:
CPU       Total     Used     Free  Buffers    Caches FreeRatio
  0     8065116  4751820  3313296     7204  1075556     41.7%

Container memory statistics are measured in KB:
CPU       Total     Used     Free  UsageRatio
  0     8065116   462672  3313296       5.7%
```

表 3-4 display memory コマンドの表示情報の説明

フィールド	説明
Memory statistics are measured in KB:	物理デバイスのメモリ使用量。以下の統計はKB単位
Mem	メモリ使用情報
Total	システムが割り当て可能な物理メモリのサイズ デバイスの物理メモリの合計は、割り当て可能な物理メモリと割り当て可能な物理メモリに分けられます。このうち、物理メモリはカーネルセグメントストア、カーネル管理オーバヘッド、 ISSU機能実行などに割り当てられない.;業務モジュールの実行、ファイル保存などの操作をサポートするために物理メモリを割り当てることができる。割り当て可能なメモリのサイズは、システムの動作に応じてデバイスが自動的に計算して決定されます。割り当て可能な物理メモリのサイズは、デバイスの物理メモリの合計から割り当て可能なメモリのサイズを引いたものです。
Used	システム全体で使用されている物理メモリのサイズ
Free	システム全体で使用可能な物理メモリのサイズ
Shared	複数のプロセスが共有する物理メモリの合計。「--」の値は、このパラメータの値の統計がサポートされていないことを示します。
Buffers	使用されているファイル・バッファのサイズ。「--」の値は、このパラメータの値の統計がサポートされていないことを示します。
Cached	キャッシュ・レジスタが使用したメモリのサイズ。「--」の値は、このパラメータの値の統計がサポートされていないことを示します。
Caches	キャッシュ・レジスタが使用したメモリサイズ
FreeRatio	システム全体の物理メモリの空き容量

フィールド	説明
-/+ buffers/cache	-/+ Buffers/Cache:used =Mem:Used –Mem:Buffers –Mem:Cachedアプリケーションが使用している物理メモリのサイズ -/+ Buffers/Cache:free =Mem:Free +Mem:Buffers +Mem:Cachedアプリケーションで使用可能な物理メモリのサイズ
Swap	パーティションの使用情報の交換
LowMem	ローエンドのメモリ使用情報
HighMem	ハイエンド・メモリの使用情報
Container memory statistics are measured in KB	Comware次のようなコンテナによるメモリの使用。 ● Total:Comwareコンテナに割り当て可能な合計物理メモリのサイズをKBで指定します。 ● Used:Comwareコンテナが使用している物理メモリのサイズをKBで指定します。 ● Free:Comwareコンテナが使用できる物理メモリのサイズをKBで指定します。 ● UsageRatio:Comwareコンテナによる物理メモリの使用

3.1.7 display memory-threshold

Syntax

display memory-threshold

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display memory-threshold コマンドを使用して、メモリ警告のしきい値に関する情報を表示します。

デバイスがすでに使用している物理メモリのサイズが、メモリの警告しきい値を超えた場合、システムはそのメモリ・タイプの例外が発生したと認識し、その例外が発生した最初の時間、最後の時間、およびその間に発生した回数を記録します。このクラスの例外の詳細については、ログ情報を参照してください。ログの概要キーワード「MEM_EXCEED_THRESHOLD」または「MEM_BELOW_THRESHOLD」で検索できます。

例

#メモリ警告しきい値に関する情報を表示します。

<Sysname> display memory-threshold

```
Memory usage threshold:100%
Free memory threshold:
Minor:512 M
Severe:448 M
Critical:384 M
Normal:576 M
Early-warning:640 M
Secure:704 M
Current memory state:Normal
Event statistics:
[Back to normal state]
First notification:0.0
Latest notification:0.0
Total number of notifications sent:0
[Enter minor low-memory state]
First notification at:0.0
Latest notification at:0.0
Total number of notifications sent:0
[Back to minor low-memory state]
First notification at:0.0
Latest notification at:0.0
Total number of notifications sent:0
[Enter severe low-memory state]
First notification at:0.0
Latest notification at:0.0
Total number of notifications sent:0
[Back to severe low-memory state]
First notification at:0.0
Latest notification at:0.0
Total number of notifications sent:0
[Enter critical low-memory state]
First notification at:0.0
Latest notification at:0.0
Total number of notifications sent:0
```

表 3-5 display memory-threshold コマンドの表示情報の説明

フィールド	説明
Memory usage threshold	メモリ使用率のしきい値

フィールド	説明
Free-memory thresholds Minor Severe Critical Normal Early-warning Secure	残りのメモリのしきい値: ● Minor:MB単位の警告レベル1 ● Severe:MB単位の二次警告しきい値 ● Critical:MB単位の3レベル警告のしきい値 ● Normal:通常の状態に戻すためのしきい値をMB単位で指定 ● Early-warning:アラート・スレッショルド、MB ● Secure:アラート・スレッショド・ステータスを回復するしきい値。単位はMBです。
Current free-memory state	システムの現在のメモリ使用状況: ● Normal:通常状態 ● Minor:1次警告しきい値の状態 ● Severe:二次アラームしきい状態 ● Critical:警告レベル3のしきい値状態 ● Normal (early-warning):ティーザー状態 ● Normal (secure):セキュリティステータス
Free-memory event statistics:	しきい値イベント統計:イベントは次のように分類されます。 ● Back to secure state:アラート前の状態に戻す ● Entered early-warning state:予告警告の状態に入る ● Back to normal state:メモリが通常の状態に戻りました。 ● Entered minor alarm state:レベル1警告のしきい値に入る ● Back to minor alarm state:1レベル警告前の状態に戻す ● Entered severe alarm state:2次アラームしきい状態に入る ● Back to severe alarm state:2次アラーム前の状態に戻す ● Entered critical alarm state:警告レベル3の状態に移行する
First notification at	イベントが最初に発生した時刻をyyyy-mm-dd hh:mm:ss.msec形式で指定します。
Latestnotification at	イベントが最後に発生した時刻をyyyy-mm-dd hh:mm:ss.msec形式で指定します。
Total number of notification send	イベントが発生した合計回数

3.1.8 display transceiver alarm

Syntax

display transceiver alarm interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number:タイプと番号でインタフェースを指定します。インタフェースを指定しない場合、このコマンドはすべてのトランシーバモジュールに存在するアラームを表示します。

説明

display transceiver alarm コマンドは、プラガブルインタフェースモジュールのアラームを表示します。

表 3-6 は、一般的なトランシーバアラームの構成要素を示しています。エラーが発生しない場合は「None」と表示されます。

表 3-6 一般的なトランシーバアラーム構成要素

フィールド	説明
APD	アバランシェフォトダイオード
PCS	物理符号化サブレイヤ
PHY XS	PHY拡張サブレイヤ
PMA/PMD	物理媒体アタッチメント部 / 物理媒体依存部
power	光出力
REFCLK	基準クロック
RX	受信
TEC	熱電冷却器
Temp	温度
TX	送信
WIS	WANインタフェースサブレイヤ

例

GigabitEthernet 1/0/1 のトランシーバモジュールに存在するアラームを表示します。

<Sysname> display transceiver alarm interface gigabitethernet 1/0/1

```
GigabitEthernet1/0/1 transceiver current alarm information:
  RX signal loss
  RX power low
```

表 3-7 display transceiver コマンドの表示情報の説明

フィールド	説明
transceiver current alarm information	トランシーバの現在のアラーム情報
RX loss of signal	受信信号損失
RX power low	受信出力低下

3.1.9 display transceiver diagnosis

Syntax

display transceiver diagnosis interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: タイプと番号でインタフェースを指定します。インタフェースが指定されていない場合、このコマンドはすべてのトランシーバモジュールのデジタル診断パラメータの現在値を表示します。

説明

display transceiver diagnosis コマンドは、トランシーバモジュール上のデジタル診断パラメータの現在値を表示します。

例

GigabitEthernet 1/0/1 のトランシーバモジュール上でデジタル診断パラメータの現在値を表示します。

<Sysname> display transceiver diagnosis interface gigabitethernet 1/0/1

```
GigabitEthernet1/0/1 transceiver diagnostic information:
  Current diagnostic parameters:
    Temp(C)  Voltage(V)  Bias(mA)  RX power(dBm)  TX power(dBm)
    36       3.31        6.13      -35.64         -5.19
  Alarm thresholds:
          Temp(C)   Voltage(V)  Bias(mA)  RX power(dBM)  TX power(dBM)
    High  50        3.55        1.44      -10.00         5.00
    Low   30        3.01        1.01      -30.00         0.00
```

表 3-8 display transceiver コマンドの表示情報の説明

フィールド	説明
transceiver diagnostic information	トランシーバモジュールのデジタル診断情報
Wave.er(nm)	波長オフセット（nm）、0.001 nm単位の精度。この項目はHPE X130 10G SFP+ LC LH80 Tunable Transceiver（JL250A）およびSFP-XG-LH80-Tunableトランシーバモジュールのみ対応しています。
Freq.er(GHz)	周波数オフセット（GHz）、0.1 GHz単位の精度。この項目はHPE X130 10G SFP+ LC LH80 Tunable Transceiver（JL250A）およびSFP-XG-LH80-Tunableトランシーバモジュールのみ対応しています。
[Module]	トランシーバモジュールのパラメータ
Temp.(C)	温度（℃）、1℃単位
Voltage(V)	電圧（V）、0.01 V単位
[Channel]	チャネル番号。チャネルはレーンとも呼ばれます。
Bias(mA)	バイアス電流（mA）、0.01 mA単位
RX power(dBm)	受信電力（dBm）、0.01 dBm単位
TX power(dBm)	送信電力（dBm）、0.01 dBm単位
TEC Curr. (%)	TEC電流（%）、0.01%単位
Laser Temp(C)	レーザー温度（℃）、0.01℃単位

3.1.10 display transceiver interface

Syntax

display transceiver interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number:インタフェースに挿入されたプラガブルインタフェースモジュールの主な機能パラメータを表示します。interface-type interface-number はインタフェースタイプとインタフェース番号を表し、このパラメータを指定しない場合はすべてのインタフェースを表します。

説明

display transceiver interface コマンドは、プラガブルインタフェースモジュールの主な機能パラメータを表示します。

例

Ten-GigabitEthernet 1/3/9 に挿入されているインタフェースモジュールの主な特性パラメータを表示します。

<Sysname> display transceiver interface Ten-GigabitEthernet 1/3/9

```
Ten-GigabitEthernet1/3/9 transceiver information:
  Transceiver Type            : STACK_SFP_PLUS
  Connector Type              : COPPER
  Wavelength(nm)              : N/A
  Transfer Distance(m)         : 1(STACK)
  Digital Diagnostic Monitoring : NO
  Vendor Name                 : Molex Inc.
  Part Number                 : 74752-1101
  Serial Number               : 008330003
```

表 3-9 display transceiver コマンドの表示情報の説明

フィールド	説明
transceiver information	プラガブルインタフェースモジュール情報
Transceiver Type	プラガブルインタフェースモジュールの物理モデル番号
Connector Type	プラガブル・インターフェース・モジュールのコネクタ・タイプ。ここで、 ● 光ファイバコネクタはSC (SC Connector、NTTが導入した抜き差しロック式光ファイバコネクタ)とLC (LC Connector、Lucent、1.25 mm/RJ45ロックアップファイバコネクタを発売)の2種類 ● その他のコネクタには、RJ-45、CX 4などがあります。
Wavelength (nm)	● 光モジュール:送信レーザーの中心波長を表示し、単位nm;複数の異なる波長の光路をサポートするモジュール(例:10 GBASE-LX4モジュール)の場合、波長の値はコンマで区切られます。 ● 電気モジュール:「N/A」と表示されます。

フィールド	説明
Transfer Distance (xx)	伝送距離は、シングルモードモジュールのxxはkm、その他のモジュールのxxはmと表示されます。モジュールが複数の伝送メディアをサポートしている場合、伝送距離の値はカンマで区切られます。距離値の後の括弧内には対応する「伝送媒体」が含まれる。各メディアの名前を次に示します。 ● 9 um:9/125 umシングルモードファイバを示します。 ● 50 um:50/125 umマルチモード光ファイバを表します。 ● 62.5 um:62.5/125 umマルチモード光ファイバを表します。 ● TP:ツイストペア ● CX 4:CX 4ケーブル用
Max power (W)	光モジュールの最大消費電力
Digital Diagnostic Monitoring	デジタル診断機能のサポート状況: ● YES:デジタル診断がサポートされていることを示します。 ● NO:デジタル診断がサポートされていないことを示します。
Vendor Name	モジュール製造またはカスタムベンダー名
Ordering Name	プラガブルインタフェースモジュールの外部モデル

3.1.11 display transceiver manuinfo

Syntax

display transceiver manuinfo interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: タイプおよび番号でインタフェースを指定します。インタフェースが指定されていない場合、このコマンドはすべてのインタフェース上のトランシーバモジュールの電子ラベル情報を表示します。

説明

display transceiver interface コマンドは、トランシーバモジュールの電子ラベル情報を表示します。

本コマンドをサポートしていないモジュールでは、以下のメッセージが表示されます。

```
The transceiver does not support this function.
```

本コマンドをサポートしていないモジュールの情報を確認するには、**display transceiver interface** コマンドを使用してください。

例

GigabitEthernet 1/0/1 のトランシーバーモジュールの電子ラベル情報を表示します。

```
<Sysname> display transceiver manuinfo interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 transceiver manufacture information:
  Manu. Serial Number : 210231A1RPN22600345K
  Manufacturing Date  : 2022-06-27
  Vendor Name         : Hisense
```

3.1.12 memory-threshold

Syntax

memory-threshold [**ratio**] **minor** *minor-value* **severe** *severe-value* **critical** *critical-value* **normal** *normal-value* [**early-warning** *early-warning-value* **secure** *secure-value*]

undo memory-threshold

デフォルト

Minor alarm threshold: 512 MB.

Severe alarm threshold: 448 MB.

Critical alarm threshold: 384 MB.

Normal state threshold: 576 MB.

Early-warning threshold: 640 MB.

Sufficient-memory threshold: 704 MB.

View

System view

定義済みユーザロール

network-admin

パラメータ

ratio:しきい値がパーセントで設定されていることを示します。このパラメータを指定しない場合は、しきい値のサイズが MB 単位で設定されていることを示します。

minor *minor-value*:1 次警告のしきい値。このパラメータの値を入力するには、次のように入力します。の結果コードが不明です。0 時に設定すると、このレベルのしきい値アラームがオフになります。

severe *severe-value*:第 2 級警告閾値。このパラメータの値を入力するには、次のように入力します。の結果コードが不明です。0 時に設定すると、このレベルのしきい値アラームがオフになります。

critical *critical-value*:3 次アラームしきい値。このパラメータの値を入力するには、次のように入力します。の結果コードが不明です。0 時に設定すると、このレベルのしきい値アラームがオフになります。

normal *normal-value*:システムメモリが正常な状態に戻ったときのメモリサイズ。このパラメータの値を入力するには、次のように入力します。の結果コードが不明です。

early-warning *early-warning-value*:アラートしきい値。このパラメータの値を入力するには、次のように入力します。の結果コードが不明です。0 時に設定すると、そのレベルのアラーム機能がオフになります。

secure *secure-value*:アラート回復しきい値。このパラメータの値を入力するには、次のように入力します。の結果コードが不明です。

説明

memory-threshold コマンドを使用して、空きメモリアラームのしきい値を設定します。

undo memory-threshold コマンドを使用して、デフォルトの状態を復元します。

システムはリアルタイムに余剰空きメモリの大きさを監視し、条件が 1 級、2 級、3 級警報閾値または正常状態回復閾値に達する時、相応の警報/警報解除通知を生成し、関連する業務モジュール/プロセスに相応の措置を取ることを通知し、最大限にメモリを利用し、また設備の正常運行を保証できる。

デバイスは、システムメモリに残っている空きメモリのサイズを監視し、**display memory** コマンドを使用してシステムメモリの使用状況を表示します。(ローエンドメモリをサポートしないデバイス)

デバイスは、ローエンドメモリに残っている空きメモリのサイズを監視し、**display memory** コマンドを使用してローエンドメモリの使用状況を表示します。(ローエンドメモリをサポートするデバイス)

ローエンドメモリをサポートするスロットの場合、デバイスはローエンドメモリに残っている空きメモリのサイズを監視します。ローエンドメモリをサポートしないスロットの場合、デバイスはシステムメモリに残っている空きメモリのサイズを監視します。**display memory** コマンドを実行し、表示メッセージに LowMem フィールドが含まれている場合は、そのスロットがローエンドメモリをサポートしていることを示します。(一部のシングルボードはローエンドメモリをサポートするデバイス)

一級、二級、三級警報のほかに、設備は警報機能をサポートする。アラート・スレッショルドは、メモリ使用率が正常範囲内にある場合に使用しますが、事前にメモリに注意を払う必要があります。アラート回復しきい値は、アラートを解除するために使用されます。

デバイスにメモリ警告が表示されたら、一時的に使用されていない設定を削除するか、メモリを解放するために一部の機能をオフにします。ただし、メモリが不足しているため、構成の一部を削除できない場合があります。

警告のしきい値の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*3 章 ハードウェアリソース管理*”を参照してください。

例

#1 次、2 次、3 次アラームしきい値をそれぞれ 64 MB、48 MB、32 MB に設定し、残りの空きメモリが 96 MB を超えると、正常な状態に戻ります。

<Sysname> system-view
[Sysname] memory-threshold minor 64 severe 48 critical 32 normal 96

#第一級、第二級、第三級警告閾値はそれぞれ設備総メモリの 3%、2%、1%であり、余剰空きメモリが設備総メモリの 5%より大きい時、正常状態に回復する。

<Sysname> system-view
[Sysname] memory-threshold ratio minor 3 severe 2 critical 1 normal 5

関連コマンド

- **display memory-threshold**

3.1.13 monitor cpu-usage enable

Syntax

monitor cpu-usage enable

undo monitor cpu-usage enable

デフォルト

CPU 使用率履歴機能がオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

monitor cpu-usage enable コマンドは、CPU 使用率履歴機能を有効にするために使用します。

undo monitor cpu-usage enable コマンドを使用して、CPU 使用率履歴機能をオフにします。

CPU 利用率履歴機能をオンにすると、一定時間(**monitor cpu-usage interval** コマンドで設定可能)ごとに CPU の利用率がサンプリングされ、サンプリング結果が履歴領域に保

存されます。これらのレコードは、**display cpu-usage history** コマンドを使用して表示でき、デバイスの最近の動作を監視できます。

例

#CPU 使用率履歴機能をオンにします。

<Sysname> system-view
[Sysname] monitor cpu-usage enable

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage interval**

3.1.14 monitor cpu-usage interval

Syntax

monitor cpu-usage interval *interval*

undo monitor cpu-usage interval

デフォルト

CPU 使用率履歴のサンプリング期間は 1 分です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:CPU 使用率の履歴は、大文字と小文字を区別せずに、5 Sec、1 Min、または 5 Min の値を取る期間で記録されます。このパラメータを入力する場合は、すべて入力してください。入力しない場合は、パラメータエラーが表示されます。

説明

monitor cpu-usage interval コマンドを使用して、CPU 使用率履歴のサンプリング期間を設定します。

undo monitor cpu-usage interval コマンドを使用して、デフォルトの状態を復元します。

CPU 利用率履歴機能をオンにすると、一定時間(**monitor cpu-usage interval** コマンドで設定可能)ごとに CPU の利用率がサンプリングされ、サンプリング結果が履歴領域に保

存されます。これらのレコードは、**display cpu-usage history** コマンドを使用して表示でき、デバイスの最近の動作を監視できます。

例

#CPU 使用率履歴のサンプリング期間を 5 秒に設定します。

<Sysname> system-view
[Sysname] monitor cpu-usage interval 5Sec

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage enable**

3.1.15 monitor cpu-usage threshold

Syntax

monitor cpu-usage threshold *severe-threshold* [**minor-threshold** *minor-threshold*]

undo monitor cpu-usage threshold [**minor-threshold**]

デフォルト

CPU 使用率アラームのしきい値は 99%です。

View

System view

定義済みユーザロール

network-admin

パラメータ

severe-threshold:CPU 使用率の高レベル警告のしきい値。値の範囲は 2~100 で、単位はパーセントです。

minor-threshold *minor-threshold*:CPU 使用率の低レベル警告のしきい値。1~「severe-threshold の構成値から 1 を引いた値」の範囲で、パーセントで指定します。このパラメータを指定しない場合、このパラメータの値は severe-threshold*0.8 になります。

説明

monitor cpu-usage threshold コマンドを使用して、CPU 使用率アラームのしきい値を設定します。

undo monitor cpu-usage threshold コマンドを使用して、デフォルトの状態を復元します。

CPU と CPU コアの使用率が 1 分ごとにサンプリングされ、サンプリングされた値がユーザ設定の警告しきい値と比較されます。サンプリング値が大きい場合は、使用率が高すぎるとみなされ、デバイスによって処理されます。

例

#CPU 使用率アラームのしきい値を 90%に設定します。

<Sysname> system-view
[Sysname] monitor cpu-usage threshold 90

関連コマンド

- **display cpu-usage configuration**

3.1.16 shutdown-interval

Syntax

shutdown-interval *interval*

undo shutdown-interval

デフォルト

ポート状態検出タイマーの時間は 30 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:ポート状態検出タイマーの時間。0~300 の範囲で秒単位で指定します。0 時の値をとり、タイミング検出を行わないことを示す。

説明

shutdown-interval コマンドを使用して、ポート状態検出タイマーの時間を設定します。

undo shutdown-interval コマンドを使用して、デフォルトの状態を復元します。

一部のプロトコルモジュールでは、特定の状況でポートが自動的にシャットダウンされます。たとえば、BPDU ガード機能がオンになっているポートが設定メッセージを受信すると、MSTP プロトコルモジュールは自動的にポートをシャットダウンします。同時に、検出タイマーが起動し、タイマーが切れるまで(time 秒が経過した後)、ポートが閉じたままになると、プロトコルモジュールは自動的にポートをアクティブにして、実際の物理状態に戻ります。

ユーザがポートタイミング検出中に検出間隔を T 1 に変更した場合、プロトコルがポートを閉じるまでの時間間隔は T に変更されます。

- T<T 1 の場合、閉じられたポートは、T 1~T の時間が経過すると再開されます。
- T>=T 1 の場合、シャットダウンされたポートはすぐに再開されます。

たとえば、現在の time が 30 に設定されていて、ポートがプロトコルモジュールによって 2 秒(T=2)シャットダウンされた後、time が 10 (T 1=10)に変更された場合、インタフェースは 8 秒後に復元されます。現在の time が 30 で、ポートがプロトコルモジュールによって 10 秒間シャットダウンされた後に time が 2 に変更された場合、ポートはすぐに復元されます。

例

#ポート状態検出タイマーの設定 100 秒。

<Sysname> system-view
[Sysname] shutdown-interval 100

3.1.17 temperature-limit

Syntax

temperature-limit slot *slot-number* { **hotspot | inflow | outflow** } *sensor-number lowlimit warninglimit* [*alarmlimit*]

undo temperature-limit slot *slot-number* **{ hotspot | inflow | outflow }** *sensor-number*

デフォルト

hotspot の lowlimit は 0

hotspot の warninglimit は 86

hotspot の alarmlimit は 89

inflow の lowlimit は 0

inflow の warninglimit は 59

inflow の alarmlimit は 64

outflow の lowlimit は 0

outflow の warninglimit は 100

outflow の alarmlimit は 117

View

System view

定義済みユーザロール

network-admin

パラメータ

slot *slot-number* : クラウドクラスタのメンバ装置のメンバ ID を指定します。

hotspot: ホットスポットセンサの温度アラームしきい値を設定します。ホットスポットセンサは、発熱しやすいチップの近くにあり、チップの監視に使用されます。

inflow: 吸気口センサの温度アラームしきい値を設定します。吸気口の近くに吸気口センサがあり、周囲温度の監視に使用されます。

outflow: 排気口センサの温度アラームしきい値を設定します。排気口の近くに排気口センサがあり、周囲温度の監視に使用されます。

sensor-number: センサを番号で指定します。値の範囲を表示するには、疑問符 (?) をこの引数の場所に入力します。

lowlimit: 低温しきい値を指定します。値の範囲は温度センサによって異なります。値の範囲を表示するには、疑問符 (?) をこの引数の場所に入力します。

warninglimit: 高温警告しきい値を指定します。このしきい値は、低温しきい値より大きくする必要があります。値の範囲を表示するには、疑問符 (?) をこの引数の場所に入力します。

alarmlimit: 高温アラームしきい値を指定します。このしきい値は、警告しきい値より大きくする必要があります。値の範囲を表示するには、疑問符 (?) をこの引数の場所に入力します。

説明

temperature-limit コマンドは温度アラームのしきい値を設定します。

undo temperature-limit コマンドはデフォルトに戻します。

しきい値の設定範囲は、CLI オンラインヘルプを使用して確認してください。

装置の温度が下限温度を下回るか、高温時のワーニング、またはアラームしきい値に到達したとき、装置は次の操作を実行します。

- ログメッセージとトラップを送信します。
- 装置の前面にある LED 表示で通知します。

例

スロット 1 内の hotspot センサ 1 の温度アラームしきい値を設定します。

<AC> system-view

[AC] temperature-limit slot 1 hotspot 1 3 76 89

目次

このセクションのページは **3-x-x** です。

4 章 NTP 4-1
4.1 NTP コマンド 4-1
4.1.1 display ntp-service sessions 4-1
4.1.2 display ntp-service status 4-6
4.1.3 display ntp-service trace 4-9
4.1.4 ntp-service acl 4-11
4.1.5 ntp-service authentication enable 4-12
4.1.6 ntp-service authentication-keyid 4-13
4.1.7 ntp-service broadcast-client 4-15
4.1.8 ntp-service broadcast-server 4-16
4.1.9 ntp-service dscp 4-17
4.1.10 ntp-service enable 4-18
4.1.11 ntp-service inbound enable 4-19
4.1.12 ntp-service max-dynamic-sessions 4-19
4.1.13 ntp-service multicast-client 4-20
4.1.14 ntp-service multicast-server 4-21
4.1.15 ntp-service reliable authentication-keyid 4-23
4.1.16 ntp-service source 4-24
4.1.17 ntp-service unicast-peer 4-25
4.1.18 ntp-service unicast-server 4-27

4章 NTP

4.1 NTPコマンド

4.1.1 display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose:NTP サービスのすべての IPv 4 セッションの詳細を表示します。このパラメータを指定しない場合は、すべてのセッションに関する簡単な情報のみが表示されます。

説明

display ntp-service sessions コマンドを使用して、NTP サービスのすべての IPv 4 セッション情報を表示します。

デバイスが NTP ブロードキャストサーバまたは NTP マルチキャストサーバとして機能している場合、デバイスで **display ntp-service sessions** コマンドを実行しても、ブロードキャストサーバまたはマルチキャストサーバに対応する NTP サービスの IPv 4 セッション情報は表示されませんが、これらのセッションは合計セッション数としてカウントされます。

例

#NTP サービスのすべての IPv 4 セッションに関する簡単な情報を表示します。

<Sysname> display ntp-service sessions

```
      source          reference       stra reach poll  now offset  delay disper
**************************************************************************
***
[12345]LOCAL(0)       LOCL             0     1   64    - 0.0000 0.0000 7937.9
   [5]0.0.0.0         INIT            16     0   64    - 0.0000 0.0000 0.0000
```

```
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

表 4-1 display ntp-service sessions コマンドの表示情報の説明

フィールド	説明
source	参照クロックがローカルクロックの場合、LOCAL (number)と表示され、ローカルクロックのアドレスが127.127.1.numberであることを示します。ここで、numberはNTPのプロセス番号で、範囲は0~3です。 基準クロックがネットワーク内の他のデバイスのクロックである場合は、タイムサーバのIPアドレスとして表示されます。このフィールドに0.0.0.0と表示されている場合は、タイムサーバのIPアドレスが解決されていません。
reference	タイムサーバの基準クロックID 基準クロックがローカルクロックの場合、このフィールドの表示はstraフィールドの値に依存します。 ● straフィールドが0または1時の場合、このフィールドはLOCLとして表示されます。 ● straフィールドが別の値の場合、このフィールドはローカルクロックのIPアドレスとして表示されます。 基準クロックがネットワーク内の他のデバイスのクロックである場合、このフィールドには、そのデバイスのIPアドレスが表示され、そのデバイスがIPv 6デバイスである場合、このフィールドには、そのデバイスのIPv 6アドレスの上位32ビットのMD 5ダイジェスト値が表示され、ドット付き十進数でダイジェスト情報が表示されます。このフィールドがINITと表示されている場合は、ローカルデバイスがタイムサーバに接続されていません。
stra	タイムサーバのクロックレイヤー数 クロック段数はクロックの正確さを決定し、 1~16の範囲で値をとり、段数が小さいほどクロックの正確さが最も高いことを示し、段数16のクロックは非同期状態である.
reach	タイムサーバの到達可能性の数。0はタイムサーバが到達不能であることを示す
poll	ポーリング間隔:2つの連続するNTPメッセージ間の秒単位の時間間隔。

フィールド	説明
now	NTPメッセージが最後に受信された時間間隔、またはローカル時刻から現在時刻に更新された時間間隔 デフォルトの単位は秒です;間隔が2048秒より長い場合は、分mと表示されます。間隔が300分を超える場合は、時間hと表示されます。間隔が96時間を超える場合は、日dとして表示されます。間隔が999日より長い場合は年y;NTPメッセージが最後に受信された場合、またはローカル時刻が現在の時刻よりも後に更新された場合は、 「-」 と表示される
offset	システムクロックの基準クロックからのミリ秒単位のクロックオフセット
delay	ローカルデバイスからタイムサーバへのラウンドトリップ遅延ミリ秒
disper	基準クロックに対するシステムクロックの最大誤差をミリ秒で指定します。
[12345]	1:システムで選択されているタイムサーバ。現在デバイスと時刻を同期しているタイムサーバです。 2:このタイムサーバのクロックレイヤー数は15以下です。 3:このタイムサーバのクロックはクロック選択アルゴリズムを通過しています 4:このタイムサーバのクロックが候補クロック 5:このタイムサーバのクロックは設定コマンドで指定されます。
Total sessions	合計セッション数

#NTP サービスのすべての IPv 4 セッションの詳細を表示します。

<Sysname> display ntp-service sessions verbose

```
Clock source:192.168.1.40
Session ID:35888
Clock stratum:2
Clock status:configured, master, sane, valid
Reference clock ID:127.127.1.0
Local mode:client, local poll interval:6
Peer mode:server, peer poll interval:6
Offset:0.2862 ms, roundtrip delay:3.2653 ms, dispersion:4.5166 ms
Root roundtrip delay:0.0000 ms root dispersion:10.910 ms
Reachabilities:31, sync distance:0.0194
Precision:2^-23, version:3, source interface:Not specified
Reftime:d17cbba5.1473de1eTue, May 17 20199:17:25.079
Orgtime:0.00000000Thu, Feb7 20196:28:16.000
Rcvtime:d17cbbc0.b1959a30Tue, May 17 20199:17:52.693
Xmttime:d17cbbc0.b1959a30Tue, May 17 20199:17:52.693
Roundtrip delay samples:0.007 0.010 0.006 0.011 0.010 0.005 0.007 0.003
```

```
Offset samples:5629.55 3913.76 5247.27 6526.92 31.99 148.72 38.27 0.29
Filter order:75260413

Total sessions:1
```

表 4-2 display ntp-service sessions verbose コマンドの表示情報の説明

フィールド	説明
Clock source	タイムサーバのIPアドレス。このフィールドに0.0.0.0と表示されている場合は、タイムサーバのIPアドレスが解決されていません。
Session ID	セッションID
Clock stratum	タイムサーバのクロックレイヤー数 クロックの精度はクロックの層数によって決まり、 1~16の範囲で値をとり、層数の値が小さいほどクロックの精度が高いことを示し、層数16のクロックは非同期状態にある.
Clock status	セッションのステータス。このフィールドの値と意味は次のとおりです。 ● configured:セッションが構成コマンドによって確立されたことを示します。 ● dynamic:セッションが動的に生成されたことを示します。 ● master:セッションに対応するタイムサーバが現在のシステムのプライマリタイムサーバであることを示します。 ● selected:セッションのタイムサーバのクロックがクロック選択アルゴリズムを通過したことを示します。 ● candidate:セッションに対応するタイムサーバのクロックが候補クロックであることを示す ● sane:セッションに対応するタイムサーバが認証され、そのタイムサーバのクロックが基準クロックとなることを示します。 ● insane:セッションに対応するタイムサーバが認証されていないか、タイムサーバは認証されているがクロックが基準クロックではないことを示します。 ● valid:セッションに対応するタイムサーバが有効であることを示す(検証、同期状態、有効なレイヤー数、ルート遅延/オフセットの非限界など) ● invalid:セッションのタイムサーバが無効であることを示します。 ● unsynced:セッションのタイムサーバのクロックが同期されていないか、レイヤー数が不正であることを示します

フィールド	説明
Reference clock ID	タイムサーバの基準クロックID このフィールドの表示は、基準クロックがローカルクロックの場合のClock stratumフィールドの値に関連しています。 ● Clock stratumフィールドの値が0または1時の場合、このフィールドはLOCLとして表示されます。 ● Clock stratumフィールドに別の値を入力すると、ローカルクロックのIPアドレスとして表示されます。 基準クロックがネットワーク内の他のデバイスのクロックである場合、このフィールドには、そのデバイスのIPアドレスが表示され、そのデバイスがIPv 6デバイスである場合、このフィールドには、そのデバイスのIPv 6アドレスの上位32ビットのMD 5ダイジェスト値が表示され、ドット付き十進数でダイジェスト情報が表示されます。このフィールドがINITと表示されている場合は、ローカルデバイスがタイムサーバに接続されていません。
Local mode	ローカルデバイスの動作モード。値は次のとおりです。 ● unspec:モードが指定されていません ● sym_active:アクティブピアモード ● sym_passive:パッシブピアモード ● client:クライアントモード ● server:サーバモード ● broadcast:ブロードキャストサーバモードまたはマルチキャストサーバモード ● bclient:ブロードキャストクライアントモードまたはマルチキャストクライアントモード
local poll interval	ローカルデバイスのポーリング間隔は、秒単位の2の累乗で表示されます。たとえば、6はポーリング間隔が2の6の累乗、つまり64 sであることを示します。
Peer mode	エンドツーエンドデバイスの動作モード。以下の値を取ります。 ● unspec:モードが指定されていません ● sym_active:アクティブピアモード ● sym_passive:パッシブピアモード ● client:クライアントモード ● server:サーバモード ● broadcast:ブロードキャストサーバモードまたはマルチキャストサーバモード ● bclient:ブロードキャストクライアントモードまたはマルチキャストクライアントモード

フィールド	説明
peer poll interval	ピアデバイスのポーリング間隔は、秒単位の2の累乗で表示されます。たとえば、6はポーリング間隔が2の6の累乗、つまり64 sであることを示します。
Offset	システムクロックの基準クロックからのミリ秒単位のクロックオフセット
roundtrip delay	ローカルデバイスからタイムサーバへのラウンドトリップ遅延ミリ秒
dispersion	基準クロックに対するシステムクロックの最大誤差
Root roundtrip delay	ローカルデバイスからプライマリタイムサーバへのラウンドトリップ遅延ミリ秒
root dispersion	マスター基準クロックからのシステムクロックの最大誤差ミリ秒
Reachabilities	タイムサーバの到達可能性の数。0はタイムサーバが到達不能であることを示す
sync distance	秒単位の誤差disperおよびラウンドトリップ遅延delayで計算された、上位のタイムサーバに対する同期距離を表します。
Precision	システムクロックの精度
version	NTPバージョン、値は1~4
source interface	ソースインタフェース。ソースインタフェースが指定されていない場合、このフィールドはNot specifiedと表示されます。
Reftime	NTPメッセージ内の参照タイムスタンプ
Orgtime	NTPメッセージの開始タイムスタンプ
Rcvtime	NTPメッセージの受信タイムスタンプ
Xmttime	NTPメッセージの送信タイムスタンプ
Roundtrip delay samples	ローカルデバイスからタイムサーバへのラウンドトリップ遅延のサンプル値
Offset samples	基準クロックに対するクロックオフセットのサンプリング値
Filter order	サンプル情報ソート
Reference clock status	ローカルクロックの動作状態。このフィールドは、ntp-service refclock-masterコマンドを使用してローカルクロックを基準クロックとして設定した場合にのみ表示されます。 ローカルクロックのreach値が255時の場合、このフィールドは working normallyになります。それ以外の場合、このフィールドの値はworking abnormallyです。
Total sessions	合計セッション数

4.1.2 display ntp-service status

Syntax

display ntp-service status

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display ntp-service status コマンドは、NTP サービスのステータス情報を表示するために使用します。

例

#時刻が同期されると、NTP サービスのステータス情報が表示されます。

<Sysname> display ntp-service status

```
Clock status:synchronized
Clock stratum:2
System peer:LOCAL (0)
Local mode:client
Reference clock ID:127.127.1.0
Leap indicator:00
NTP version:4
Clock jitter:0.000977 s
Stability:0.000 pps
Clock precision:2^-23
Root delay:0.00000 ms
Root dispersion:3.96367 ms
Reference time:d0c5fc32.92c70b1eWed, Dec 29 2019 18:28:02.573
System poll interval:256 s
```

#時刻が同期されていない場合は、NTP サービスのステータス情報が表示されます。

<Sysname> display ntp-service status

```
Clock status:unsynchronized
Clock stratum:16
Reference clock ID:none
Clock jitter:0.000000 s
Stability:0.000 pps
Clock precision:2^-23
Root delay:0.00000 ms
Root dispersion:2e-05 ms
Reference time:d0c5fc32.92c70b1eWed, Dec 29 2019 18:28:02.573
System poll interval:8 s
```

表 4-3 display ntp-service status コマンドの表示情報の説明

フィールド	説明
Clock status	システム時間のステータス。値は次のとおりです。 ● synchronized:システム時刻が同期されました ● unsynchronized:システム時刻が同期していません
Clock stratum	システムクロックの階層数
System peer	システムクロック:選択されたタイムサーバのIPアドレス
Local mode	選択したタイムサーバに対するローカルデバイスの動作モードには、次の値があります。 ● unspec:モードが指定されていません ● sym_active:アクティブピアモード ● sym_passive:パッシブピアモード ● client:クライアントモード ● server:サーバモード ● broadcast:ブロードキャストサーバモードまたはマルチキャストサーバモード ● bclient:ブロードキャストクライアントモードまたはマルチキャストクライアントモード
Reference clock ID	基準クロックID **1.** IPv4 NTP サーバの場合: ローカルデバイスがリモートタイムサーバから時刻同期を取得する場合、リモートサーバのIPアドレスを表します。 ローカルデバイスがローカルクロックから時刻同期を取得する場合は、ローカルクロックのIDを表します。 ● ローカルクロックのレイヤ数は1時で、LOCLとして表示されます。 ● ローカルクロックの層数が他の値の場合、ローカルクロックのIPアドレスとして表示される. **2.** IPv6 NTP サーバの場合: ローカルデバイスがリモートタイムサーバから時刻同期を取得するときに、リモートサーバのIPv 6アドレスの上位32ビットを表すMD 5ダイジェスト値 ローカルデバイスがローカルクロックから時刻同期を取得する場合は、ローカルクロックのIDを表します。 ● ローカルクロックのレイヤ数は1時で、LOCLとして表示されます。 ● ローカルクロックの層数が他の値の場合、ローカルクロックのIPv 6アドレスの上位32ビットのMD 5ダイジェスト値として表示される.

フィールド	説明
Leap indicator	アラーム状態は、次の値を取ります。 • 00:通常状態 • 01:うるう秒のフラグ。1日の最後の分が61秒であることを示します。 • 10:1日の最後の分が59秒であることを示すうるう秒フラグ • 11:時刻が同期されていない警告状態
NTP version	選択した時刻サーバのNTPバージョン。1~4の値をとり、時刻が同期されている場合にのみ表示されます。
Clock jitter	システムクロックの基準クロックからのオフセット (秒単位)
Stability	クロック周波数の安定性は、値が小さいほど安定します
Clock precision	システムクロックの精度
Root delay	ローカルデバイスからプライマリタイムサーバへのラウンドトリップ遅延ミリ秒
Root dispersion	マスター基準クロックからのシステムクロックの最大誤差ミリ秒
Reference time	基準タイムスタンプ
System poll interval	システムポーリング間隔 (秒)

4.1.3 display ntp-service trace

Syntax

display ntp-service trace [**source** *interface-type interface-number*]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

source *interface-type interface-number*:プライマリタイムサーバのバックトラック時にNTP メッセージを送信する送信元インタフェースを指定します。interface-type interface-number はインタフェースのタイプとインタフェース番号を示します。ローカルデバイスが NTP メッセージをタイムサーバに送信する場合、メッセージの送信元アドレスは、指定された送信元インタフェースのプライマリ IPv 4 アドレスです。NTP タイムサーバアドレスがリンクローカルアドレスの場合、メッセージの送信元アドレスは、メッセージ送信インタフェースのリンクローカルアドレスです。このパラメータが指定されていない

場合、プライマリ時刻サーバをバックトラックするときに NTP メッセージを送信する送信元インタフェースとして、メッセージ送信インタフェースが使用されます。

説明

display ntp-service trace コマンドを使用すると、ローカルデバイスからプライマリタイムサーバにバックトラックされる各 NTP タイムサーバに関する簡単な情報を表示できます。

送信元インタフェースを指定してプライマリタイムサーバをバックトラックする場合は、プライマリタイムサーバおよび各 NTP タイムサーバと送信元インタフェース間のルートが到達可能であることを確認する必要があります。そうしないと、バックトラックが失敗します。

例

#ローカルデバイスからプライマリタイムサーバにバックトラックされる各 NTP タイムサーバの簡単な情報を表示します。

<Sysname> display ntp-service trace

```
Server     127.0.0.1
Stratum    3, jitter  0.000, synch distance 0.0000.
Server     3000::32
Stratum    2 , jitter 790.00, synch distance 0.0000.
RefID      127.127.1.0
```

上の情報はサーバ 127.0.0.1 の同期チェーンを示します:サーバ 127.0.0.1 はサーバ 3000::32 に同期し、サーバ 3000::32 はローカルクロックから同期します。

表 4-4 display ntp-service trace コマンドの表示情報の説明

フィールド	説明
Server	タイムサーバのIPアドレス
Stratum	対応するサーバのクロックレイヤー数を表します。
jitter	1つ上のクロックからのクロック偏差を表す2乗平均平方根。単位は秒です。
synch distance	秒単位の誤差disperおよびラウンドトリップ遅延delayで計算された、上位のタイムサーバに対する同期距離を表します。
RefID	プライマリタイムサーバのID。プライマリ基準クロックの階層数は0時で、LOCLとして表示されます。その他の値の場合は、プライマリ基準クロックのIPアドレスが表示されます。

関連コマンド

- **ntp-service source**
- **ntp-service unicast-server**
- **ntp-service unicast-peer**

4.1.4 ntp-service acl

Syntax

ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv4-acl-number*]

デフォルト

ピアデバイスは、ローカルデバイスの NTP サービスへのアクセスを peer に制御します。

View

System view

定義済みユーザロール

network-admin

パラメータ

peer:フルアクセス。この権限は、ローカルデバイスに対するローカルデバイスの時刻の同期、ローカルデバイスに対する制御クエリ(アラーム情報、認証ステータス、タイムサーバ情報など、NTP のステータスを照会します。)、およびローカル・デバイスとピアの時刻の同期を許可する。

query:クエリを制御する権限のみがあります。この権限は、ローカルデバイスの NTP サービスに対する制御クエリを許可するだけで、ローカルデバイスの時刻と同期することはできません。

server:サーバアクセスおよびクエリ権限。このパーミッションは、ローカルデバイスへの時間同期を許可し、ローカルデバイスへの制御クエリを実行しますが、ローカルデバイスはローカルデバイスへの時間同期を行いません。

synchronization:サーバへのアクセス権のみを持ちます。このパーミッションでは、ローカルデバイスとの時間同期だけが許可されますが、制御クエリは実行できません。

ipv4-acl-number:参照する ACL を番号で指定します(Access Control List、アクセス制御リスト#アクセスセイギョリスト#)。ACL でフィルタリングされたピアデバイスには、このコマンドで指定されたアクセス制御パーミッションがあります。ipv4-acl-number は、IPv4 基本 ACL または拡張 ACL の番号で、範囲は 2000~2999 と 3000~3999 です。

説明

ntp-service acl コマンドは、ローカルデバイスの NTP サービスへのピアデバイスのアクセス制御を設定します。

undo ntp-service acl コマンドは、設定されたアクセス制御パーミッションを取り消すために使用します。

NTP サービスへのアクセス制御は、peer、server、synchronization、query の順になります。デバイスが NTP サービス要求を受信すると、最初に一致した権限がデバイスのアクセス制御権限である、権限の高い順に一致します。一致するパーミッションがなければ、

ローカルデバイスとの時間同期、ローカルデバイスへの制御クエリ、ローカルデバイスとの時間同期は許可されません。

参照 ACL が存在しない場合、どのデバイスもローカル NTP サービスにアクセスできます。参照 ACL にルールが設定されていない場合、どのデバイスもローカル NTP サービスにアクセスできません。

ntp-service acl コマンドは最小限のセキュリティ対策を提供し、より安全な方法は認証です。

例

#設定 10.10.0.0/16 ネットワークセグメントのピアデバイスは、ローカルデバイスにフルアクセスできます。

<Sysname> system-view
[Sysname] acl basic 2900
[Sysname-acl-ipv4-basic-2900] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2900] quit
[Sysname] ntp-service peer acl 2900

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

4.1.5 ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

デフォルト

NTP 認証機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

ntp-service authentication enable コマンドを使用して、NTP 認証機能を有効にします。

undo ntp-service authentication enable コマンドを使用して、NTP 認証機能をオフにします。

セキュリティ要件の高い一部のネットワークでは、NTP プロトコルを実行するときに NTP 認証を有効にする必要があります。クライアント側とサーバ側の認証により、クライアントが認証を通過したデバイスのみと時刻同期を行うことを保証し、クライアントが不正なサーバから誤った時刻同期情報を取得することを回避する。

NTP 認証が有効になっている場合は、認証キーを設定して信頼されたキーに設定しても、正しく認証されます。

例

#NTP 認証をオンにします。

<Sysname> system-view
[Sysname] ntp-service authentication enable

関連コマンド

- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

4.1.6 ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode** { **hmac-sha-1** | **hmac-sha-256** | **hmac-sha-384** | **hmac-sha-512** | **md5** } { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number*] *

undo ntp-service authentication-keyid *keyid*

デフォルト

NTP 認証キーが設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid:1~4294967295 の範囲で認証キーを識別するキー番号。

authentication-mode:検証アルゴリズムを示す。

hmac-sha-1:認証に HMAC-SHA-1 アルゴリズムが使用されることを示します。

hmac-sha-256:認証に HMAC-SHA-256 アルゴリズムが使用されることを示します。

hmac-sha-384:認証に HMAC-SHA-384 アルゴリズムが使用されることを示します。

hmac-sha-512:認証に HMAC-SHA-512 アルゴリズムが使用されることを示します。

md 5:MD 5 アルゴリズムによる認証を示します。

cipher:キーを暗号化テキストとして設定します。

simple:キーをクリアテキストで設定します。このキーは暗号化テキストとして保存されます。

string:キー文字列。大文字と小文字が区別されます。平文鍵は 1~32 文字の文字列、暗号文鍵は 1~73 文字の文字列である。

acl *ipv4-acl-number*:エンドツーエンドデバイスの ACL フィルタリング。ACL でフィルタリングされたピアデバイスには、このキーID を使用して認証する権限があります。ipv4-acl-number は IPv 4 ベース ACL の番号で、範囲は 2000~2999 です。

説明

ntp-service authentication-keyid コマンドを使用して、NTP 認証キーを設定します。

undo ntp-service authentication-keyid コマンドを使用して、指定した NTP 認証キーを削除します。

セキュリティ要件の高い一部のネットワークでは、NTP プロトコルを実行するときに認証を有効にする必要があります。クライアント側とサーバ側の認証により、クライアントが認証されたデバイスとだけ時刻同期を行うことを保証し、時刻同期の安全性を向上させる。

NTP プロトコルがどのキーを使用してピアを認証するかは、ピアメッセージに含まれるキーID によって決まります。これにより、ピアの認証時にキーが正しいかどうかだけが問題となり、ピアがキーID を使用する権限を持っているかどうかは問題となりません。acl パラメータを使用して、このキーID を使用して認証する権限を持つピアデバイスを指定します。次の点に注意してください。

- acl パラメータは、ローカルで NTP セッションを確立する必要がある場合、またはすでにピアが存在する場合に、ピアにそのキーID を使用する権限があるかどうかをさらに確認します。
- 参照先の ACL が存在しない場合、どのデバイスでもこのキーID を使用してローカル側で認証できます。
- 参照されている ACL にルールが設定されていない場合、デバイスはこのキーID を使用してローカル側で認証できません。

クライアントとサーバの両方で同じキーID、認証アルゴリズム、およびキー値を設定し、そのキーID を使用して認証する権限がピアにあることを確認する必要があります。そうしないと、時刻同期が行われません。

NTP 認証キーを構成した後、**ntp-service reliable authentication-keyid** コマンドを使用して信頼されたキーに設定する必要もあります。NTP 認証キーが信頼できるキーとして指定されている場合、キーを削除すると、そのキーは自動的に信頼できないキーになり、**undo ntp-service reliable authentication-keyid** コマンドを実行する必要がなくなります。

5 つの認証アルゴリズムのセキュリティは、HMAC-SHA-512、HMAC-SHA-384、HMAC-SHA-256、HMAC-SHA-1、MD 5 です。

このコマンドを繰り返し実行することで、複数の NTP 認証キーを構成できます。デバイスには、最大 128 個の NTP 認証キーを設定できます。

例

#MD 5 認証キーを設定し、キーID 番号 10、キーBetterKey をクリアテキストで入力します。

<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey

関連コマンド

- **ntp-service authentication enable**
- **ntp-service reliable authentication-keyid**

4.1.7 ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

デフォルト

NTP 動作モードが設定されていません。

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service broadcast-client コマンドを使用して、NTP ブロードキャストクライアントモードで動作するようにデバイスを設定し、現在のインタフェースを使用して NTP ブロードキャストメッセージを受信します。

undo ntp-service broadcast-client コマンドは、NTP ブロードキャストクライアントモードの設定を解除するために使用します。

デバイスが NTP ブロードキャストクライアントモードで動作するように設定すると、デバイスは NTP ブロードキャストサーバから送信された NTP ブロードキャストメッセージをインタフェースで受信し、受信したメッセージに基づいて時刻同期を行います。

デバイスがブロードキャストクライアントモードで動作するようにインタフェースが設定されている場合は、そのインタフェースを集約グループに含めないことをお勧めしま

す。インタフェースを集約グループに参加させる場合は、最初に NTP ブロードキャストクライアントの設定を解除することをお勧めします。

例

#設定デバイスはブロードキャストクライアントモードで動作し、VLAN インタフェース 1 で NTP ブロードキャストメッセージを受信します。

<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-client

関連コマンド

- **ntp-service broadcast-server**

4.1.8 ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

デフォルト

NTP 動作モードが設定されていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

authentication-keyid *keyid*:NTP メッセージをブロードキャストクライアントに送信するときに、指定されたキーを使用してメッセージのダイジェストを計算するように指定します。keyid 1~4294967295 の範囲で値を指定できます。このパラメータが指定されていない場合、認証が有効になっているブロードキャストクライアントをローカルデバイスで同期できません。

version *number*:NTP バージョン番号を指定します。number は 1~4 の範囲の値を取り、デフォルト値は 4 です。

説明

ntp-service broadcast-server コマンドを使用して、NTP ブロードキャストサーバモードで動作するようにデバイスを設定し、現在のインタフェースを使用して NTP ブロードキャストメッセージを送信します。

undo ntp-service broadcast-server コマンドは、NTP ブロードキャストサーバモードの設定を解除するために使用します。

NTP ブロードキャストサーバモードで動作するようにデバイスを設定すると、デバイスはそのインタフェースを介してブロードキャストアドレス 255.255.255.255 に NTP メッセージを定期的に送信します。

デバイスがブロードキャストサーバモードで動作するようにインタフェースが設定されている場合は、そのインタフェースを集約グループに含めないことをお勧めします。インタフェースを集約グループに参加させる場合は、最初に NTP ブロードキャストサーバの設定を解除することをお勧めします。

例

#設定デバイスはブロードキャストサーバモードで動作し、VLAN インタフェース 1 で NTP ブロードキャストメッセージを送信し、キー番号 4 で暗号化し、NTP バージョン番号を 4 に設定します。

<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 4

関連コマンド

- **ntp-service broadcast-client**

4.1.9 ntp-service dscp

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

デフォルト

NTP メッセージの DSCP 優先度は 48 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value:NTP メッセージの DSCP 優先度。範囲は 0~63 です。

説明

ntp-service dscp コマンドを使用して、NTP メッセージの DSCP プライオリティを設定します。

undo ntp-service dscp コマンドを使用して、デフォルトの状態を復元します。

DSCP は IP メッセージ中の ToS フィールドを持ち、メッセージ自体の優先順位を表し、メッセージ転送の優先度を決定する。

例

#NTP メッセージの DSCP プライオリティを 30 に設定します。

<Sysname> system-view
[Sysname] ntp-service dscp 30

4.1.10 ntp-service enable

Syntax

ntp-service enable

undo ntp-service enable

デフォルト

NTP サービスが停止しています。

View

System view

定義済みユーザロール

network-admin

説明

ntp-service enable コマンドは、NTP サービスを開始するために使用します。

undo ntp-service enable コマンドは、NTP サービスをシャットダウンするために使用します。

例

#NTP サービスをオンにします。

<Sysname> system-view
[Sysname] ntp-service enable

4.1.11 ntp-service inbound enable

Syntax

ntp-service inbound enable

undo ntp-service inbound enable

デフォルト

インタフェースは NTP メッセージを受信しています。

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service inbound enable コマンドを使用して、NTP メッセージを受信するインタフェースを有効にします。

undo ntp-service inbound enable コマンドは、NTP メッセージを受信するインタフェースの機能を停止するために使用します。

デバイスがインタフェースの対応するネットワークセグメント内のピアデバイスに時刻同期を提供できない場合、またはデバイスがインタフェースの対応するネットワークセグメント内のピアデバイスから時刻同期を取得できない場合は、インタフェースで **undo ntp-service inbound enable** コマンドを実行して、インタフェースが NTP メッセージの受信をオフにすることができます。

例

#VLAN インタフェース 1 の NTP メッセージ受信機能をオフにします。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] undo ntp-service inbound enable
```

4.1.12 ntp-service max-dynamic-sessions

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

デフォルト

NTP 動的セッションの最大数は 100 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

number:NTP 動的セッションの最大数。範囲は 0~100 です。

説明

ntp-service max-dynamic-sessions コマンドを使用して、NTP 動的セッションの最大数を設定します。

undo ntp-service max-dynamic-sessions コマンドを使用して、デフォルトの状態を復元します。

同じデバイスに同時に存在するセッションの数は最大 128 で、これには静的セッションと動的セッションが含まれます。静的セッションは、ユーザが NTP 関連のコマンドを手動で構成して確立したセッションです。ダイナミックセッションは、NTP の実行中に確立される一時セッションです。

この構成を使用すると、動的セッションの数を制限して、デバイスに過剰な動的セッションが保持され、システムリソースが過剰に消費されないようにすることができます。

例

#NTP 動的セッションの最大数を 50 に設定します。

<Sysname> system-view
[Sysname] ntp-service max-dynamic-sessions 50

関連コマンド

- **display ntp-service sessions**

4.1.13 ntp-service multicast-client

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

デフォルト

NTP 動作モードが設定されていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address:NTP メッセージのマルチキャスト IP アドレス。デフォルトは 224.0.1.1 です。マルチキャストクライアントとマルチキャストサーバで設定されるマルチキャストアドレスは同じである必要があります。

説明

ntp-service multicast-client コマンドを使用して、NTP マルチキャストクライアントモードで動作するようにデバイスを設定し、現在のインタフェースを使用して NTP マルチキャストメッセージを受信します。

undo ntp-service multicast-client コマンドは、NTP マルチキャストクライアントモードの設定を解除するために使用します。

NTP マルチキャストクライアントモードで動作するようにデバイスを設定すると、デバイスは指定されたマルチキャストアドレスの宛先アドレスを持つ NTP メッセージをインタフェースで受信し、受信したメッセージに基づいて時刻同期を行います。

デバイスがマルチキャストクライアントモードで動作するようにインタフェースが設定されている場合は、そのインタフェースを集約グループに参加させないことをお勧めします。インタフェースを集約グループに参加させる場合は、最初に NTP マルチキャストクライアントの設定を解除することをお勧めします。

例

#設定デバイスはマルチキャストクライアントモードで動作し、VLAN インタフェース 1 で宛先アドレス 224.0.1.1 の NTP メッセージを受信します。

<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ntp-service multicast-client 224.0.1.1

関連コマンド

- **ntp-service multicast-server**

4.1.14 ntp-service multicast-server

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

デフォルト

NTP 動作モードが設定されていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address:NTP メッセージのマルチキャスト IP アドレス。デフォルトは 224.0.1.1 です。マルチキャストクライアントとマルチキャストサーバで設定されるマルチキャストアドレスは同じである必要があります。

authentication-keyid *keyid*:マルチキャストクライアントに NTP メッセージを送信するときに、指定されたキーを使用するように指定しますメッセージのダイジェストを計算します。keyid 1~4294967295 の範囲で値を指定できます。このパラメータが指定されていない場合、認証が有効になっているマルチキャストクライアントをローカルデバイスで同期できません。

ttl *ttl-number*:マルチキャストメッセージの存続期間を指定します。ttl-number は 1~255 の値を取り、デフォルト値は 16 です。

version *number*:NTP バージョン番号を指定します。number は 1~4 の範囲の値を取り、デフォルト値は 4 です。

説明

ntp-service multicast-server コマンドを使用して、NTP マルチキャストサーバモードで動作するようにデバイスを設定し、現在のインタフェースを使用して NTP マルチキャストメッセージを送信します。

undo ntp-service multicast-server コマンドは、NTP マルチキャストサーバモードの設定を解除するために使用します。

NTP マルチキャストサーバモードで動作するようにデバイスを設定すると、デバイスはそのインタフェースを介して、指定されたマルチキャストアドレスに NTP メッセージを定期的に送信します。

デバイスがマルチキャストサーバモードで動作するようにインタフェースが設定されている場合は、そのインタフェースを集約グループに参加させないことをお勧めします。インタフェースを集約グループに参加させる場合は、最初に NTP マルチキャストサーバの設定を解除することをお勧めします。

例

#設定デバイスはマルチキャストサーバモードで動作し、VLAN インタフェース 1 で NTP メッセージを送信します。NTP メッセージの宛先アドレスはマルチキャストアドレス 224.0.1.1 で、NTP メッセージはキー番号 4 で暗号化され、NTP バージョン番号は 4 に設定されます。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
```

[Sysname-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 4 authentication-keyid 4

関連コマンド

- **ntp-service multicast-client**

4.1.15 ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

デフォルト

信頼されたキーが指定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid:1~4294967295 の範囲のキー番号。

説明

ntp-service reliable authentication-keyid コマンドを使用して、作成したキーが信頼されていることを指定します。

undo ntp-service reliable authentication-keyid コマンドは、信頼されたキーを取り消すために使用します。

認証を有効にすると、クライアントは信頼されたキーを提供するサーバとのみ時刻同期を行います。サーバによって提供されたキーが信頼されていない場合、クライアントはそのキーと同期しません。

このコマンドを設定する前に、認証スイッチがオンになっていてキーが設定されていること、つまりキーが存在することを確認してから、キーが信頼できるかどうかを設定します。NTP 認証キーが信頼できるキーとして指定されている場合、キーを削除すると、そのキーは自動的に信頼できないキーになり、undo ntp-service reliable authentication-keyid コマンドを実行する必要がなくなります。

このコマンドは複数回設定でき、最大 128 個の信頼できるキーを設定できます。

例

#NTP 認証を有効にします。設定番号 37 のキーは MD 5 アルゴリズムで認証され、キー値は BetterKey です。

<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey

#このキーが信頼されたキーであることを指定します。

[Sysname] ntp-service reliable authentication-keyid 37

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**

4.1.16 ntp-service source

Syntax

ntp-service source { *interface-type interface-number* | *ipv4-address* }

undo ntp-service source

デフォルト

NTP メッセージの送信元 IPv 4 アドレスが指定されていない場合、デバイスはルーティングテーブルに基づいてメッセージの送信インタフェースを検索し、送信インタフェースのプライマリ IPv 4 アドレスを NTP メッセージの送信元 IPv 4 アドレスとして使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number:インタフェースタイプとインタフェース番号。NTP メッセージの送信元インタフェースを表します。NTP メッセージの送信元インタフェースを指定した場合、デバイスは、NTP メッセージをアクティブに送信するときに、指定した送信元インタフェースのプライマリ IPv 4 アドレスをメッセージの送信元アドレスに設定します。NTP 応答メッセージは、このアドレスを宛先アドレスに設定します。

ipv4-address:NTP メッセージの送信元 IPv 4 アドレス。

説明

ntp-service source コマンドを使用して、NTP メッセージの送信元 IPv 4 アドレスを指定します。

undo ntp-service source コマンドを使用して、デフォルトの状態を復元します。

機器が受信した NTP 要求メッセージに対して応答を行う場合、応答メッセージの送信元アドレスはつねに NTP 要求メッセージを受信した宛先アドレスとなる。

ローカルデバイス上の他のインタフェースの IP アドレスが応答メッセージの宛先アドレスにならないようにするには、このコマンドを使用します。

このコマンドを使用して NTP メッセージのソース IPv 4 アドレスを指定する場合は、次の点に注意してください。

- NTP がクライアント/サーバモードで動作している場合、コマンド **ntp-service unicast-server** で NTP メッセージのソース IPv 4 アドレスを指定した場合は、コマンド **ntp-service unicast-server** で指定したソース IPv 4 アドレスが使用されます。
- NTP がピアモードで動作している場合、コマンド **ntp-service unicast-peer** で NTP メッセージの送信元 IPv 4 アドレスを指定した場合は、コマンド **ntp-service unicast-peer** で指定した送信元 IPv 4 アドレスが優先されます。
- NTP がマルチキャストモードで動作しているときに、Interface view で **ntp-service multicast-server** コマンドが設定されている場合、NTP マルチキャストメッセージの送信元 IPv 4 アドレスは、**ntp-service multicast-server** コマンドが設定されているインタフェースです。
- NTP がブロードキャストモードで動作しているときに、Interface view で **ntp-service broadcast-server** コマンドが設定されている場合、NTP ブロードキャストメッセージの送信元 IPv 4 アドレスは、**ntp-service broadcast-server** コマンドが設定されているインタフェースです。
- 指定された NTP ソース IPv 4 アドレスが down の場合、デバイスは NTP メッセージを送信しなくなります。

例

#VLAN 1 インタフェースの IP アドレスを NTP メッセージの送信元 IPv 4 アドレスとして設定します。

```
<Sysname> system-view
[Sysname] ntp-service source vlan-interface 1
```

4.1.17 ntp-service unicast-peer

Syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer { *peer-name* | *ip-address* }

デフォルト

パッシブピアが指定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

peer-name:パッシブピアのホスト名。1~253 文字の文字列で、大文字と小文字は区別されません。

ip-address:パッシブピアの IP アドレス。このアドレスは、ユニキャストアドレスのみにすることができ、ブロードキャストアドレス、マルチキャストアドレス、またはローカルクロックの IP アドレスにすることはできません。

authentication-keyid *keyid*:ピアに NTP メッセージを送信するときに、指定したキーを使用してメッセージのダイジェストを計算するように指定します。keyid 1~4294967295 の範囲で値を指定できます。このパラメータを指定しない場合、ローカルデバイスとピア間の認証は行われません。

maxpoll *maxpoll-interval*:最大ポーリング間隔を設定します。maxpoll-interval は 4~17 の範囲で、最大ポーリング間隔は 2 の maxpoll-interval 乗で、最大ポーリング間隔は 24~217 (16~131072)秒の範囲です。このパラメータのデフォルト値は 6 で、最大ポーリング間隔は 64 秒です。

minpoll *minpoll-interval*:最小ポーリング間隔を設定します。minpoll-interval は 4~17 の範囲で、最大ポーリング間隔は maxpoll-interval の 2 乗で、最大ポーリング間隔は 24~217 (16~131072)秒の範囲です。このパラメータのデフォルト値は 6 で、最小ポーリング間隔は 64 秒です。

priority: [ピア] では、ip-address または peer-name で指定されたピアが同期ピアとして優先されます。

source *interface-type interface-number*:NTP メッセージの送信元インタフェースを指定します。ローカルデバイスが NTP メッセージをピアに送信する場合、メッセージの送信元アドレスは、指定された送信元インタフェースのプライマリ IP アドレスになります。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。このパラメータが指定されていない場合は、ルーティングテーブルに基づいてメッセージの発信インタフェースが検索され、発信インタフェースのプライマリ IP アドレスが NTP メッセージの送信元 IP アドレスとして使用されます。

version *number*:NTP バージョン番号を指定します。number は 1~4 の範囲の値を取り、デフォルト値は 4 です。

説明

ntp-service unicast-peer コマンドを使用して、デバイスのパッシブピアを指定します。

undo ntp-service unicast-peer コマンドを使用して、デバイスに指定されたパッシブピアを削除します。

デバイスにパッシブピアを指定すると、アクティブピアとパッシブピアの時間を同期できます。両方のクロックが同期状態であれば、レイヤ数の大きいクロックはレイヤ数の小さいクロックの時刻に同期する。

アクティブピアは、ポーリングと呼ばれるプロセスで、パッシブピアと定期的に時間同期します。このコマンドの maxpoll パラメータと minpoll パラメータを使用して、NTP ピアモードのシステムポーリング間隔の最大値と最小値を設定します。ピアを選択すると、デバイスは最小ポーリング間隔でポーリングを行います。同期時間エラーがシステムの許容範囲内で安定している場合、ポーリング間隔は最大値まで徐々に大きくなります。同期時間の誤差がシステムで許容される範囲を複数回超え続けると、ポーリング間隔が短くなります。

ポーリング間隔の変更はすぐには有効にならず、次回のポーリング時に有効になります。

例

#設定デバイスはアクティブピアモードで動作し、パッシブピアの IP アドレスは 10.1.1.1、NTP バージョン番号は 4、NTP メッセージの送信元インタフェースは VLAN インタフェース 1 です。

<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 4 source vlan-interface 1

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

4.1.18 ntp-service unicast-server

Syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server { *server-name* | *ip-address* }

デフォルト

NTP サーバが指定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

server-name:NTP サーバのホスト名。1~253 文字の文字列で、大文字と小文字は区別されません。

ip-address:NTP サーバの IP アドレス。このアドレスは、ユニキャストアドレスのみにすることができ、ブロードキャストアドレス、マルチキャストアドレス、またはローカルクロックの IP アドレスにすることはできません。

authentication-keyid *keyid*:NTP サーバにメッセージを送信するときに、指定したキーを使用してメッセージのダイジェストを計算するように指定します。keyid 1~4294967295 の範囲で値を指定できます。このパラメータを指定しない場合、ローカルデバイスと NTP サーバ間の認証は行われません。

maxpoll *maxpoll-interval*:最大ポーリング間隔を設定します。maxpoll-interval は 4~17 の範囲で、最大ポーリング間隔は 2 の maxpoll-interval 乗で、最大ポーリング間隔は 24~217 (16~131072)秒の範囲です。このパラメータのデフォルト値は 6 で、最大ポーリング間隔は 64 秒です。

minpoll *minpoll-interval*:最小ポーリング間隔を設定します。minpoll-interval は 4~17 の範囲で、最大ポーリング間隔は maxpoll-interval の 2 乗で、最大ポーリング間隔は 24~217 (16~131072)秒の範囲です。このパラメータのデフォルト値は 6 で、最小ポーリング間隔は 64 秒です。

priority:サーバが同等の条件で優先されるように指定します。

source *interface-type interface-number*:NTP メッセージの送信元インタフェースを指定します。ローカルデバイスが NTP メッセージをサーバに送信する場合、メッセージの送信元アドレスは、指定された送信元インタフェースのプライマリ IP アドレスです。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。このパラメータが指定されていない場合は、ルーティングテーブルに基づいてメッセージの発信インタフェースが検索され、発信インタフェースのプライマリ IP アドレスが NTP メッセージの送信元 IP アドレスとして使用されます。

version *number*:NTP バージョン番号を指定します。number は 1~4 の範囲の値を取り、デフォルト値は 4 です。

説明

ntp-service unicast-server コマンドは、デバイスの NTP サーバを指定します。

undo ntp-service unicast-server コマンドを使用して、デバイスに指定された NTP サーバを削除します。

デバイスに NTP サーバを指定すると、デバイスはそのサーバの時刻と同期できますが、サーバはデバイスの時刻と同期しません。

NTP クライアントは、ポーリングと呼ばれる周期的に NTP サーバに時刻を同期します。このコマンドの maxpoll パラメータと minpoll パラメータを使用して、NTP クライアントサーバモードのシステムポーリング間隔の最大値と最小値を設定します。NTP サーバを選択すると、デバイスは最小ポーリング間隔でポーリングを行います。同期時間エラーがシステムの許容範囲内で安定した後、ポーリング間隔は最大値まで徐々に大きくなります。同期時間の誤差がシステムで許容される範囲を複数回超え続けると、ポーリング間隔が短くなります。

ポーリング間隔の変更はすぐには有効にならず、次回のポーリング時に有効になります。

例

#デバイスの NTP サーバを 10.1.1.1、バージョン番号 4 に設定します。

<Sysname> system-view
[Sysname] ntp-service unicast-server 10.1.1.1 version 4

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

目次

このセクションのページは **3-x-x** です。

5 章 Information Center 5-1
5.1 Information Center コマンド 5-1
5.1.1 character-set 5-1
5.1.2 display info-center 5-2
5.1.3 display logbuffer 5-4
5.1.4 display logbuffer summary 5-6
5.1.5 display logfile buffer 5-7
5.1.6 display logfile summary 5-8
5.1.7 enable log updown 5-9
5.1.8 info-center enable 5-9
5.1.9 info-center loghost keep-alive custom-info 5-10
5.1.10 info-center loghost keep-alive enable 5-11
5.1.11 info-center loghost keep-alive interval 5-12
5.1.12 info-center loghost keep-alive level 5-13
5.1.13 info-center logbuffer 5-14
5.1.14 info-center logbuffer size 5-15
5.1.15 info-center logfile directory 5-15
5.1.16 info-center logfile enable 5-16
5.1.17 info-center logfile frequency 5-17
5.1.18 info-center logfile size-quota 5-18
5.1.19 info-center loghost 5-19
5.1.20 info-center loghost source 5-20
5.1.21 info-center source 5-21
5.1.22 info-center synchronous 5-23
5.1.23 info-center syslog min-age 5-24
5.1.24 info-center timestamp 5-25
5.1.25 info-center timestamp loghost 5-26
5.1.26 logfile save 5-27
5.1.27 reset logbuffer 5-28
5.1.28 snmp-agent trap enable syslog 5-28
5.1.29 terminal debugging 5-29
5.1.30 terminal logging level 5-30
5.1.31 terminal monitor 5-31
5.1.32 timestamp 5-32

5章 Information Center

5.1 Information Centerコマンド

5.1.1 character-set

Syntax

character-set { **gb18030** | **utf-8** }

undo character-set

デフォルト

ログには GB 18030 文字セットエンコーディングが使用されます。

View

Log output profile view

定義済みユーザロール

network-admin

Parameters

gb18030: GB 18030 文字セット符号化方式を指定します。

utf-8: UTF-8 文字セット符号化方式を指定します。

説明

ログの文字セットエンコーディングを指定するには、**character-set** を使用します。

undo character-set を使用して、デフォルトに戻します。

ユーザのログイン端末が端末から受信したログメッセージに漢字を正しく表示するには、端末と同じ文字セット符号化方式を使用する必要があります。

このコマンドを使用して、ログの UTF-8 または GB 18030 文字セットエンコーディングを指定できます。

例

#ログ出力プロファイル profile 1 を作成し、ログの UTF-8 文字セットエンコーディングを指定する。

<AC> system-view
[AC] info-center output-profile profile1
[AC-ic-profile-profile1] character-set utf-8

5.1.2 display info-center

Syntax

display info-center

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display info-center コマンドは、各出力方向の情報を表示します。

例

#各出力方向の情報を表示します。

<AC> display info-center

```
Information Center:Enabled
Console:Enabled
Monitor:Enabled
Log host:Enabled
192.168.0.1, log output filter:loghost1,
port number:5000, DSCP value:0, host facility:local7
Log buffer:Enabled
Max buffer size 1024、current buffer size 512、
Current messages 0、dropped messages 0、overwritten messages 0
Log file:Enabled
Security log file:Enabled
Information timestamp format:
Log host:Date
Other output destination:Date
```

表 5-1 display info-center コマンドの表示情報の説明

フィールド	説明
Information Center	情報センターの現在の状態: • Enabled:ログの出力が許可されていることを示します。 • Disabled:出力ログが無効であることを示します。

フィールド	説明
Console	コンソール方向の現在の状態: • Enabled:コンソールへのログ出力が許可されていることを示します。 • Disabled:コンソールへのログ出力が禁止されていることを示します。
Monitor	端末方向の現在の状態を監視する。 • Enabled:監視端末へのログ出力が許可されていることを示す • Disabled:監視端末へのログ出力が禁止されていることを示す
Log host:Enabled 192.168.0.1, log output filter:loghost1, port number:5000, DSCP value:0, host facility:local7	ホストの向きに関する情報をログに記録します。 • Enabled:ログホストへのログ出力が許可されていることを示します。ログをログホストに出力できるようにすると、ユーザの構成に応じて、次の情報も表示されます。 ○ ログホストの IP アドレス ○ 関連するログ出力ルールの名前 ○ ログホストがログ情報を受信するポート ○ ログメッセージの DSCP 優先順位 ○ ログホストのログツール • Disabled:ログホストへのログ出力が禁止されていることを示します。
Log buffer:Enabled Max buffer size 1024、 current buffer size 512、 Current messages 0、 dropped messages 0、 overwritten messages 0	オープン状態、最大容量、現在の容量、現在の情報数、破棄された情報数、上書きされた情報数など、ログバッファの方向に関する情報
Log file	ログファイルの方向の現在の状態: • Enabled:ログファイルへのログ出力が許可されていることを示します。 • Disabled:ログファイルへのログ出力が禁止されていることを示します。
Security log file	セキュリティログファイルの方向現在の状態: • Enabled:セキュリティログファイルへのログ出力が許可されていることを示します。 • Disabled:ログがセキュリティログファイルに出力されないことを示します。

フィールド	説明
Information timestamp format: Loghost:Date Other output destination:Date	情報タイムスタンプ構成。ログホスト出力方向と非ログホスト出力方向を含みます。ログ情報のタイムスタンプのタイプは、boot、date、iso、none、no-year-dateの5つです。

5.1.3 display logbuffer

Syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize*] * [**last-mins** *mins*]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

reverse:新しいログから古いログへの順序を指定します。このパラメータを指定しない場合、古いログが最初に表示され、最後に最新のログが表示されます。

level *severity*:ログ・キャッシュ内の指定したレベルのログに関する情報を表示します。severity は情報のレベルを示し、0~7 の範囲の値をとります。このパラメータを指定しないと、syslog バッファ内のすべてのレベルのログ情報が表示されます。

表 5-2 情報レベル・リスト

数値	情報レベル	説明
0	emergency	システム認証が期限切れなど、デバイスが使用できないことを示す情報
1	alert	デバイスに重大な障害が発生し、トラフィックがインタフェースの上限を超えた場合などに即座に対応する必要があることを示す情報
2	critical	デバイスの温度がアラーム値を超えている、デバイスの電源、ファンに障害が発生しているなどの重大な情報を示します。
3	error	インタフェースリンクの状態の変化などのエラーメッセージを示します。
4	warning	インタフェース接続の切断、メモリ不足の警告などの警告メッセージを表示

数値	情報レベル	説明
5	notification	端末からのデバイスへのログイン、デバイスの再起動など、通常は発生するが重要な情報を示します。
6	informational	コマンドラインからコマンドを入力した場合のログ情報、pingコマンドを実行した場合のログ情報など、ログに記録する必要があることを示す通知情報
7	debugging	デバッグ・プロセスによって生成された情報を示します。

size *buffersize*:ログバッファ内の指定した数の最新ログを表示します。buffersize は、表示するログバッファ内の最新のログ情報の数を示し、1~10240 の値を取ります。このパラメータを指定しないと、システム・ログ・バッファ内のすべてのログ情報が表示されます。

last-mins *mins*:最近のログバッファのステータスとログバッファに記録されたログ情報を分単位で 1~43200 の範囲で表示するように指定します。このパラメータを指定しない場合、表示される情報は時間フィルタリングされません。

説明

display logbuffer コマンドを使用して、ログバッファのステータスとログバッファに記録されたログ情報を表示します。

例

#syslog バッファのステータスと、バッファに記録されたログ情報を表示します。

<AC> display logbuffer

```
Log buffer:Enabled
Max buffer size:1024
Actual buffer size:5 12
Dropped messages:0
Overwritten messages:718
Current messages:5 12
%Jun 17 15:57:09:578 2019 AC SYSLOG/7/SYS_RESTART:System restarted --
…
```

#過去 5 分間のログバッファの状態とログバッファに記録されたログ情報を表示します。

<AC> display logbuffer last-mins 5

```
Log buffer:Enabled
Max buffer size:1024
Actual buffer size:5 12
Dropped messages:0
Overwritten messages:0
Current messages:191
%Jan1 01:00:06:784 2019 AC SHELL/6/SHELL_CMD:-Line=vty0-IPAddr=192.168.1.242-
User =**;Command is display current-configuration
```

```
%Jan1 01:03:19:691 2019 AC SHELL/5/SHELL_LOGIN:VTY logged in from 192.168.1.33.
%Jan1 01:03:21:269 2019 AC SHELL/6/SHELL_CMD:-Line=vty1-IPAddr=192.168.1.33-
User =**;Command is display logbuffer last-mins 5
```

表 5-3 display logbuffer コマンドの表示情報の説明

フィールド	説明
Log buffer	ログバッファ方向への出力を許可するかどうか: • Enabled:許可 • Disabled:許可されていないことを示す
Max buffer size	許可されているログバッファに格納できる情報の最大数
Actual buffer size	現在構成されているログバッファに格納できる情報の最大数
Dropped messages	廃棄された情報の数(メモリ割当てに失敗したか、ログバッファの割当てに時間がかかり、失われた情報の数)
Overwritten messages	上書きされる情報の数(バッファ・ストレージが不足すると、最初に受信した情報の数が新しい情報で上書きされます。)
Current messages	現在記録されている情報の数
Failed to obtainthe specified data.The following tries to display all data in the logbuffer.	(デバイスの内部データベース情報との相互作用の例外)表示情報の取得に失敗しました。ログバッファ内のすべてのデータを表示します。

関連コマンド

- **info-center logbuffer**
- **reset logbuffer**

5.1.4 display logbuffer summary

Syntax

display logbuffer summary [**level** *severity*]

View

すべての View

定義済みユーザロール

network-admin

network-operator

パラメータ

level *severity*:ログ・キャッシュ内の指定したレベルのログのサマリー情報を表示します。severity は情報レベルを示し、0~7 の値をとります。表 5-2 を参照してください。このパ

ラメータを指定しないと、システム・ログ・バッファ内のすべてのレベルのログ・サマリー情報が表示されます。

例

#syslog バッファの概要を表示します。

<AC> display logbuffer summary

```
EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
    0     0     0     0    22     0     1     0
```

表 5-4 display logbuffer summary コマンドの表示情報の説明

フィールド	説明
EMERG	emergency レベルの情報の数。表 5-2
ALERT	alert レベルの情報の数。表 5-2
CRIT	critical レベルの情報の数。表 5-2
ERROR	error レベルの情報の数。表 5-2
WARN	warning レベルの情報の数。表 5-2
NOTIF	notification レベルの情報の数。表 5-2
INFO	informational レベルの情報の数。表 5-2
DEBUG	debugging レベルの情報の数。表 5-2

5.1.5 display logfile buffer

Syntax

display logfile buffer

View

すべての View

定義済みユーザロール

network-admin

network-operator

説明

display logfile buffer コマンドは、ログファイルバッファの内容を表示します。

ログは、ログファイルに保存される前に、一時的にログファイルバッファにキャッシュされます。ログの保存が自動的または手動でトリガーされるまで、ログファイルバッファの内容はログファイルに保存されません。保存に成功すると、ログファイルバッファの内容が空になります。

例

#ログファイルバッファの内容を表示します。

<AC> display logfile buffer

```
%@356%Dec 13 16:53:45:495 2019 QX-W2300AC シリーズ SHELL/6/SHELL_CMD:-Line=con
0-IPAddr =**- User =**;Command is logfile save.
```

関連コマンド

- **info-center logfile frequency**
- **logfile save**

5.1.6 display logfile summary

Syntax

display logfile summary

View

すべての View

定義済みユーザロール

network-admin

network-operator

例

#ログファイルの設定を表示します。

<AC> display logfile summary

```
Log file:Enabled.
Log file size quota:10 MB
Log file directory:flash:/logfile
Writing frequency:24 hour 0 min 10 sec
```

表 5-5 display logfile summary コマンドの表示情報の説明

フィールド	説明
Log file	ログファイルの出力方向を許可するかどうか: • Enabled:オンになっていることを示します。 • Disabled:オンになっていないことを示します。
Log file size quota	1つのログファイルに使用できるストレージの最大サイズをMB単位で指定します。
Log file directory	ログファイルが保存されているパス
Writing frequency	ログファイルが自動的に保存される頻度

5.1.7 enable log updown

Syntax

enable log updown

undo enable log updown

デフォルト

すべてのポートが、状態が変化したときにポート Link up と Link down のログ情報を生成できるようにします。

View

Interface view

定義済みユーザロール

network-admin

説明

enable log updown コマンドは、状態が変化したときにポートが Link up と Link down のログ情報を生成できるようにするために使用します。

undo enable log updown コマンドは、状態が変化したときにポートが Link up と Link down のログ情報を生成しないようにするために使用します。

例

#ポート GigabitEthernet1/0/1 が Link up と Link down のログ情報を生成しないようにします。

<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] undo enable log updown

5.1.8 info-center enable

Syntax

info-center enable

undo info-center enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center enable コマンドを使用して、情報センター機能をオンにします。

undo info-center enable コマンドを使用して、情報センター機能をオフにします。

例

#情報センター機能をオンにします。

<AC> system-view
[AC] info-center enable
Information center is enabled.

5.1.9 info-center loghost keep-alive custom-info

🕮 **メモ**：

このコマンドは、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

Syntax

info-center loghost keep-alive custom-info *text*

undo info-center loghost keep-alive custom-info

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

text: カスタム情報を 1 から 255 文字の文字列で指定します。

説明

info-center loghost keep-alive custom-info コマンドはキープアライブログに含めるカスタム情報を設定します。

undo info-center loghost keep-alive custom-info コマンドはデフォルトに戻します。

キープアライブログにカスタム情報を含めることで、ログ解析やトラブルシューティングを容易にします。

カスタム情報には、デバイスの設置位置、デバイス ID、その他備考の情報を含めることができます。

カスタム情報には ASCII 文字のみ設定できます。特殊文字は使用できません。

例

キープアライブログにカスタム情報として No.123 を設定します。

<AC> system-view

[AC] info-center loghost keep-alive custom-info No.123

関連コマンド

- **info-center loghost keep-alive enable**
- **info-center loghost keep-alive interval**
- **info-center loghost keep-alive level**

5.1.10 info-center loghost keep-alive enable

🕮 **メモ：**

このコマンドは、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

Syntax

info-center loghost keep-alive enable

undo info-center loghost keep-alive enable

デフォルト

ソフトウェアバージョン 9.6.05d を含む以前のソフトウェアでは有効。

ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアでは無効。

View

System view

定義済みユーザロール

network-admin

説明

info-center loghost keep-alive enable コマンドはキープアライブログ送信を有効にします。

undo info-center loghost keep-alive enable コマンドはデフォルトに戻します。

この機能を有効にすると、装置は設定された全てのログホストに対して定期的にキープアライブログを送信します。

キープアライブログを定期的に受信することにより、装置の運用状態を確認できるようにします。

例

キープアライブログの送信を有効にします。

<AC> system-view

[AC] info-center loghost keep-alive enable

関連コマンド

- **info-center loghost**
- **info-center loghost keep-alive interval**
- **info-center loghost keep-alive level**
- **info-center loghost keep-alive message**

5.1.11 info-center loghost keep-alive interval

🕮 **メモ**:

このコマンドは、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

Syntax

info-center loghost keep-alive interval *seconds*

undo info-center loghost keep-alive interval

デフォルト

60 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

seconds: キープアライブログを送信する間隔を 60 から 3600 秒の範囲で指定します。

説明

info-center loghost keep-alive interval コマンドはキープアライブログ送信間隔を設定します。

undo info-center loghost keep-alive interval コマンドはデフォルトに戻します。

例

キープアライブログの送信間隔を 180 秒に設定します

<AC> system-view

[AC] info-center loghost keep-alive interval 180

5.1.12 info-center loghost keep-alive level

🕮 **メモ：**

このコマンドは、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

Syntax

info-center loghost keep-alive level *severity*

undo info-center loghost keep-alive level

デフォルト

Informational

View

System view

定義済みユーザロール

network-admin

パラメータ

severity: キープアライブログのレベルを、alert、critical、debugging、emergency、error、informational、notification、warning のいずれかで指定します。

説明

info-center loghost keep-alive level コマンドはキープアライブログのレベルを設定します。

undo info-center loghost keep-alive level コマンドはデフォルトに戻します。

装置は指定されたレベルでキープアライブログをログホストへ送信します。

例

キープアライブログのレベルを notification に設定します

<AC> system-view

[AC] info-center loghost keep-alive level notification

関連コマンド

- **info-center loghost keep-alive enable**
- **info-center loghost keep-alive interval**
- **info-center loghost keep-alive message**

5.1.13 info-center logbuffer

Syntax

info-center logbuffer

undo info-center logbuffer

デフォルト

ログ情報をログバッファに出力できるようにします。

View

System view

定義済みユーザロール

network-admin

説明

info-center logbuffer コマンドは、ログ情報をログバッファに出力できるようにするために使用します。

undo info-center logbuffer コマンドは、ログ情報がログバッファに出力されないようにするために使用します。

例

#ログ情報をログバッファに出力できるように設定します。

<AC> system-view
[AC] info-center logbuffer

関連コマンド

- **display logbuffer**
- **info-center enable**

5.1.14 info-center logbuffer size

Syntax

info-center logbuffer size *buffersize*

undo info-center logbuffer size

デフォルト

ログバッファには、512 個の情報を格納できます。

View

System view

定義済みユーザロール

network-admin

パラメータ

buffersize:ログバッファに格納できる情報の数。範囲は 0~1024 で、デフォルト値は 512 です。

説明

info-center logbuffer size コマンドを使用して、ログバッファに格納できる情報の数を設定します。

undo info-center logbuffer size コマンドを使用して、デフォルトの状態を復元します。

例

#ログバッファに格納できる情報の数を 50 個に設定します。

<AC> system-view
[AC] info-center logbuffer size 50

#回復ログバッファに格納できる情報の数は 512 個です。

<AC> system-view
[AC] undo info-center logbuffer size

関連コマンド

- **display logbuffer**
- **info-center enable**

5.1.15 info-center logfile directory

Syntax

info-center logfile directory *dir-name*

デフォルト

ログファイルを格納するディレクトリは、デバイスのデフォルトのファイルシステムルートにある logfile フォルダです。

View

System view

定義済みユーザロール

network-admin

パラメータ

dir-name:ログファイルを格納するパス。1~64 文字の文字列。

説明

info-center logfile directory コマンドは、ログファイルを格納するディレクトリを構成します。

構成を実行する前に、ログファイルを格納するディレクトリは、現在作成されているディレクトリである必要があります。

生成されるログファイルのサフィックス名は.log です。

設定はデバイスの再起動後に無効になります。

例

#ログファイルを格納するディレクトリを flash:/test に設定します。

<AC> mkdir test

```
Creating directory flash:/test ...Done.
```

<AC> system-view

[AC] info-center logfile directory flash:/test

関連コマンド

- **info-center logfile enable**

5.1.16 info-center logfile enable

Syntax

info-center logfile enable

undo info-center logfile enable

デフォルト

ログ情報をログファイルに出力できるようにします。

View

System view

定義済みユーザロール

network-admin

例

#ログ情報をログファイルに出力できるように設定します。

<AC> system-view
[AC] info-center logfile enable

5.1.17 info-center logfile frequency

Syntax

info-center logfile frequency *freq-sec*

undo info-center logfile frequency

デフォルト

デバイスがログファイルを自動的に保存する頻度は 86400 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

freq-sec:ログファイルが自動的に保存される頻度。1~86400 の範囲で秒単位で指定します。

説明

info-center logfile frequency コマンドは、システムがログファイルを自動的に保存する頻度を設定します。

undo info-center logfile frequency コマンドを使用して、デフォルトの状態を復元します。

ログファイルを自動的に保存する頻度を設定すると、指定した頻度でログファイルバッファの内容がログファイルに書き込まれます。

例

#デバイスがログファイルを自動的に保存する頻度を 6 万秒に設定します。

<AC> system-view

[AC] info-center logfile frequency 60000

関連コマンド

- **info-center logfile enable**

5.1.18 info-center logfile size-quota

Syntax

info-center logfile size-quota *size*

undo info-center logfile size-quota

デフォルト

1 つのログファイルに使用できるストレージ容量は最大 10 MB です。

View

System view

定義済みユーザロール

network-admin

パラメータ

size:1 つのログファイルで使用できるストレージ領域の最大値。1~10 の範囲で、単位は MB です。

説明

info-center logfile size-quota コマンドを使用して、1 つのログファイルで使用できる最大ストレージ容量を設定します。

undo info-center logfile size-quota コマンドを使用して、デフォルトの状態を復元します。

例

#1 つのログファイルに使用できるストレージの最大サイズを 6 MB に設定します。

<AC> system-view
[AC] info-center logfile size-quota 6

関連コマンド

- **info-center logfile enable**

5.1.19 info-center loghost

Syntax

info-center loghost { *hostname* | *ipv4-address* } [**port** *port-number*] [**dscp** *dscp-value*] [**facility** *local-number*] [**filter** *filter-name*] [**output-profile** *profile-name*]

undo info-center loghost { *hostname* | *ipv4-address* }

デフォルト

ログホストと関連パラメータが構成されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

hostname:ログのホスト名を 1~253 文字の文字列で指定します。大文字と小文字は区別されず、文字、数字、 「-」 、 「_」 、 「.」 を使用できます。

ipv4-address:ログホストの IPv 4 アドレスを指定します。

port *port-number*:ログホストがログ情報を受信するポート番号を 1~65535 の範囲で指定します。デフォルト値は 514 です。このパラメータの値は、ログホスト側の構成と一致する必要があります。一致しない場合、ログホストはログ情報を受信できません。

dscp *dscp-value*: ログメッセージの DSCP (Differentiated Services Code Point 、Differentiated Services コードポイント)優先度を 0~63 の範囲で指定します。デフォルトは 0 です。値が大きいほど優先度が高くなります。DSCP 優先度は、IP メッセージ内の ToS フィールドにカプセル化され、デバイスがメッセージ送信の優先度を決定できる、メッセージ自体の優先度を表します。

facility *local-number*:ログホストのロギングツールを設定します。範囲は local0~local7 で、デフォルト値は local7 です。主にログホスト側で異なるログソースをマークし、対応するログソースのログを見つけ、フィルタリングします。

filter *filter-name*:ログホストに関連付けられたログ出力ルールの名前を指定します。ルールに一致するログのみが対応するログホストに出力されます。filter-name は、ログ情報出力ルールの名前を示す 1~8 文字の文字列で、大文字と小文字は区別されません。このパラメータを指定しない場合は、ログ出力ルールとして info-center source コマンドログのホスト方向の設定が使用されます。

output-profile *profile-name*: ログホストへのログ出力を制御するログ出力プロファイルを指定します。profile-name 引数は、大文字と小文字を区別しない 1~8 文字の文字列です。ログ出力プロファイルを指定しない場合、デバイスはデフォルトのパラメータを使用してログを出力します。

説明

info-center loghost コマンドを使用して、ログホストと関連パラメータを設定します。

undo info-center loghost コマンドは、ログホストと関連パラメータの設定を解除するために使用します。

設定 **info-center loghost** コマンドは、**info-center enable** コマンドを使用して情報センター機能を有効にした場合にのみ有効になります。

例

#IP アドレス 1.1.1.1 のログホストにログ情報を送信するようにシステムを設定します。

<AC> system-view
[AC] info-center loghost 1.1.1.1

関連コマンド

- **info-center filter**
- **info-center source**

5.1.20 info-center loghost source

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

デフォルト

送信されるログ情報の送信元 IP アドレスとして、送信側のプライマリ IP アドレスが使用されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number:ログ情報を送信する送信元 IP アドレスに対応する出力インタフェースのタイプと番号を指定します。

説明

info-center loghost source コマンドは、送信されるログ情報の送信元 IP アドレスを設定します。

undo info-center loghost source コマンドを使用して、デフォルトの状態を復元します。

ログ情報の送信元 IP アドレスを設定すると、ログ情報の送信元 IP アドレスは、実際に使用されている物理インタフェースに関係なく、指定したインタフェースのプライマリ IP アドレスになります。

設定 **info-center loghost source** コマンドは、**info-center enable** コマンドを使用して情報センター機能を有効にした場合にのみ有効になります。

例

#送信するログ情報の送信元 IP アドレスとして Loopback0 の IP アドレスを使用するように設定します。

<AC> system-view
[AC] interface loopback 0
[AC-LoopBack0] ip address 2.2.2.2 32
[AC-LoopBack0] quit
[AC] info-center loghost source loopback 0

5.1.21 info-center source

Syntax

info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** } { **deny** | **level** *severity* }

undo info-center source { *module-name* | **default** } { **console** | **logbuffer** | **logfile** | **loghost** | **monitor** }

デフォルト

ログ情報の出力ルール表 5-6 を参照してください。

表 5-6 ログ情報のデフォルト出力ルール

出力方向	ログ情報のソース	スイッチ	等級
コンソール	サポートされているすべてのモジュール	有効	debugging
監視端末	サポートされているすべてのモジュール	無効	debugging
ログホスト	サポートされているすべてのモジュール	有効	informational
ログバッファ	サポートされているすべてのモジュール	有効	informational
ログファイル	サポートされているすべてのモジュール	有効	informational

View

System view

定義済みユーザロール

network-admin

パラメータ

module-name:アプリケーションモジュールのログ情報を指定する出力ルールを設定します。システムでサポートされているソース・モジュールは、System view で info-center source ?に表示されます。

default:すべてのアプリケーションモジュールのログ情報のデフォルト出力ルールを設定します。

console:コンソールに出力します。

logbuffer:ログバッファに出力します。

logfile:ログファイルに出力します。

loghost:ログホストへの出力。

monitor:監視端末への出力。

deny:メッセージの出力を禁止します。

level *severity*:情報レベルを 0~7 の範囲で指定します。表 5-2 を参照してください。このパラメータを使用して、出力できるログ情報の最小レベルを制御できます。

説明

info-center source コマンドは、ログ情報の出力ルールを設定します。

undo info-center source コマンドは、デフォルトに戻します。

module-name パラメータを使用してアプリケーションモジュールの出力ルールを個別に設定していない場合、モジュールは **default** パラメータで設定された出力ルールを使用します。**default** パラメータを使用して出力ルールを設定してしない場合、デフォルトの出力ルールが使用されます。

出力ルールをアプリケーションモジュールに個別に設定した場合、*module-name* パラメータを使用してルールを変更または削除する必要があります。**default** パラメータを使用した新しい設定は、出力ルールを個別に設定したアプリケーションモジュールでは有効になりません。

module-name パラメータを使用して同じアプリケーションモジュールの出力ルールを複数回設定した場合、最後に実行したコマンドが有効になります。

default パラメータを使用してデフォルトの出力ルールを複数回設定した場合、最後に実行されたコマンドが有効になります。

例

#VLAN モジュールの情報だけがコンソールに出力され、emergency のログ情報が出力されます。

<AC> system-view
[AC] info-center source default console deny
[AC] info-center source vlan console level emergency

#前述の例に基づいて、コンソール方向の VLAN モジュールの出力を取り消します(すべての情報がコンソールに表示されない)。

<AC> system-view
[AC] undo info-center source vlan console

5.1.22 info-center synchronous

Syntax

info-center synchronous

undo info-center synchronous

デフォルト

コマンドライン入力エコー機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

info-center synchronous コマンドは、コマンドライン入力エコー機能を有効にします。

undo info-center synchronous コマンドは、コマンドライン入力エコー機能をオフにします。

コマンドライン、パラメータ、または Y/N 確認情報を入力するときに、大量のログ情報によって中断されると、入力した文字列と必要な文字列がわからなくなることがあります。コマンドライン入力エコー機能を使用して、ユーザの設定を支援します。ログ情報の出力が完了すると、ユーザの既存の入力または Y/N 確認メッセージがエコーされ、ユーザは構成を続行できます。

例

#デバイスのコマンドライン入力エコー機能をオンにし、display current-configuration コマンドを入力してデバイスの現在の設定を表示します。

<AC> system-view
[AC] info-center synchronous
Info-center synchronous output is on
[AC] display current-

このとき、ログメッセージを受信すると、システムはすべてのログメッセージが表示された後、ユーザの入力(この例は、「display current-」です。)を付加して表示する。

```
%May 21 14:33:19:425 2019 AC SHELL/5/SHELL_LOGIN:VTY logged in from
192.168.1.44
```

[AC] display current-

この時点で、ユーザは configuration (コマンド display current-configuration の完全な入力を完了します。)を入力し続け、コマンドを実行します。

#デバイスのコマンドライン入力エコー機能をオンにして、現在の設定(対話情報の入力)を保存します。

<AC> system-view

[AC] info-center synchronous

```
Info-center synchronous output is on
```

[AC] save

```
The current configuration will be written to the device.Are you sure?[Y/N]:
```

この時点で、ログ情報を受信すると、すべてのログメッセージが表示された後、[Y/N]:が追加で表示されます。

```
%May 21 14:33:19:425 2019 AC SHELL/5/SHELL_LOGIN:VTY logged in from 192.168.1.44
[Y/N]:
```

このとき、ユーザは Y または N を入力してログ情報出力前の動作を継続することができる。

5.1.23 info-center syslog min-age

Syntax

info-center syslog min-age *min-age*

undo info-center syslog min-age

デフォルト

ログ情報の最小保存時間が設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

min-age:ログ情報の最小保存時間を示し、 1~8760 の範囲の値をとり、単位は時間である。

説明

info-center syslog min-age コマンドを使用して、ログ情報の最小保存時間を設定します。

undo info-center syslog min-age コマンドを使用して、デフォルトの状態を復元します。

例

#ログ情報の最小保存時間を 168 時間に設定します。

<AC> system-view
[AC] info-center syslog min-age 168

5.1.24 info-center timestamp

Syntax

info-center timestamp { **boot** | **date** | **none** }

undo info-center timestamp

デフォルト

タイムスタンプ出力形式は date です。

View

System view

定義済みユーザロール

network-admin

パラメータ

boot:システムが起動してからの経過時間。xxx.yyy の形式で指定します。xxx はシステムが起動してからの経過時間をミリ秒で表したものです。32 桁高い場合は yyy、32 桁低い場合は 0.21990989 のようになります(Jun 25 14:09:26:881 2019 と同等)。

date:Dec のように「MMM DD hh:mm:ss:ms YYYY」の形式で、システムの現在の日付と時刻 8 10:12:21:708 2019。

- 「MMM」は、Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec の英語の月の略語です。
- 「DD」は日付を表し、値が 10 未満の場合は「7」のように「スペース+日付」の形式になります。
- 「hh:mm:ss:ms」はローカル時間を表し、 hh は 0023, mm と ss はともに 0059, ms は 0~999 の範囲で値をとる。
- 「YYYY」は年を表します。

none:時刻情報なし。

説明

info-center timestamp コマンドは、コンソール、監視端末、ログバッファ、およびログファイルの方向に送信されるログ情報のタイムスタンプ出力形式を設定します。

undo info-center timestamp コマンドを使用して、デフォルトの状態を復元します。

例

#ログ情報の設定タイムスタンプ出力形式は boot 形式です。

<AC> system-view
[AC] info-center timestamp boot

関連コマンド

- **info-center timestamp loghost**

5.1.25 info-center timestamp loghost

Syntax

info-center timestamp loghost { **date** [**with-milliseconds**] | **iso** [**with-milliseconds** | **with-timezone**] * | **no-year-date** | **none** }

undo info-center timestamp loghost

デフォルト

ログホスト宛のログ情報のタイムスタンプ出力形式は date 形式です。

View

System view

定義済みユーザロール

network-admin

パラメータ

date:タイムスタンプ出力形式を Dec のように MMM DD hh:mm:ss YYYY に設定します。8 10:12:21 2019 ですが、最終的な表示形式はログホストによって決定されます。

iso:タイムスタンプ出力形式を、2019-09-21 T 15:32:55 のような ISO 8601 標準形式に設定します。

with-milliseconds:タイムスタンプがミリ秒まで正確で、ミリ秒が標準のポイント番号で区切られていることを示します。date 形式のタイムスタンプの場合は、Dec 8 10:12:21.708 2019 のようにミリ秒が付加されます。iso 形式のタイムスタンプの場合は、2019-09-21 T 15:32:55.708 のようにミリ秒が付加されます。このパラメータを指定しない場合は、タイムスタンプが秒単位で表示されます。

with-timezone:タイムスタンプには、2019-09-21 T 15:32:55+01:00 のようなタイムゾーン情報が含まれます。このパラメータを指定しない場合は、タイムスタンプにタイムゾーン情報が含まれていません。

no-year-date:システムの現在の日付と時刻。ただし、年とミリ秒の情報は含まれません。

none:時刻情報なし。

説明

info-center timestamp loghost コマンドを使用して、ログホストに送信されるログ情報のタイムスタンプ出力形式を設定します。

undo info-center timestamp loghost コマンドを使用して、デフォルトの状態を復元します。

例

#ログホストに送信されるログ情報のタイムスタンプを no-year-date 形式に設定します。

<AC> system-view
[AC] info-center timestamp loghost no-year-date

関連コマンド

- **info-center timestamp**

5.1.26 logfile save

Syntax

logfile save

View

すべての view

定義済みユーザロール

network-admin

説明

logfile save コマンドは、ログファイルバッファの内容をすべて手動でログファイルに保存します。

ログファイルの保存パスは、**info-center logfile directory** コマンドで設定できます。

ログファイルが正常に保存されると、ログファイルバッファの内容は空になります。

このコマンドの実行時にログファイルバッファにログが存在しない場合、このコマンドは正常に実行されますが、既存のログファイルは作成または更新されません。

例

#ログファイルバッファの内容を手動でログファイルに保存します。

<AC> logfile save
The contents in the log file buffer have been saved to the file flash:/logfile/logfile.log.

関連コマンド

- **info-center logfile enable**

- **info-center logfile directory**

5.1.27 reset logbuffer

Syntax

reset logbuffer

View

User view

定義済みユーザロール

network-admin

説明

reset logbuffer コマンドは、ログバッファから情報をクリアするために使用します。

例

#ログバッファの情報をクリアします。

<AC> reset logbuffer

関連コマンド

- **display logbuffer**

5.1.28 snmp-agent trap enable syslog

Syntax

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

デフォルト

システムログは、警告メッセージとして送信されません。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable syslog コマンドを使用して、システムログを警告メッセージ送信用にカプセル化します。

undo snmp-agent trap enable syslog コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定すると、デバイスは出力ルールに基づいて各方向にログを出力するだけでなく、ログ情報を SNMP モジュールとログ警告バッファにカプセル化します。

- SNMP モジュールに送信後、宛先ホストに出力するか、Trap または Inform として送信するかは、SNMP モジュールの構成によって決まります。アラーム情報および SNMP 構成の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。
- ログ警告バッファに送信された後、ユーザは「ログアラームバッファに対応する MIB ノード」を使用して、ログ情報でカプセル化された警告情報を直接読み取ることができます。**info-center syslog trap buffersize** コマンドを使用して、ログ警告バッファのサイズを設定することもできます。

例

#システムログを警告メッセージ送信用にカプセル化します。

<AC> system-view
[AC] snmp-agent trap enable syslog

関連コマンド

- **info-center syslog trap buffersize**

5.1.29 terminal debugging

Syntax

terminal debugging

undo terminal debugging

デフォルト

現在のエンドポイントにデバッグ情報を出力できません。

View

User view

定義済みユーザロール

network-admin

説明

terminal debugging コマンドは、デバッグ情報を現在の端末に出力できるようにするために使用します。

undo terminal debugging コマンドを使用すると、デバッグ情報が現在の端末に出力されなくなります。

デバッグ情報とは、業務モジュールのデバッグ情報スイッチを入れると、業務モジュールが生成する debugging レベルのログ情報である。

コンソールにデバッグ情報を表示する必要がある場合は、情報センター機能(情報センター機能はデフォルトで有効になっています)を有効にする前に **terminal debugging** コマンドを設定し、最後に **debugging** コマンドを使用して機能モジュールのデバッグ情報スイッチをオンにします。

モニタリングターミナルでデバッグ情報を表示する必要がある場合は、InfoCenter 機能(情報センター機能はデフォルトで有効になっています)を有効にする前に **terminal monitor** および **terminal debugging** コマンドを設定し、最後に **debugging** コマンドを使用して機能モジュールのデバッグ情報スイッチをオンにします。

このコマンドは、現在の接続に対してのみ有効であることに注意してください。端末がデバイスに再接続すると、このコマンドはデフォルトに戻ります。

terminal logging level 7 コマンドまたは **terminal debugging** コマンドを実行すると、現在のターミナルがデバッグ情報を表示できるようになりますが、次の点が異なります。

- **terminal logging level 7** コマンドを実行すると、現在のターミナルでは、レベル 0~7 のすべてのログを出力できます。
- **terminal debugging** コマンドを実行すると、現在のエンドポイントは、**terminal logging level** コマンドで設定されたログ情報とレベル 7 のデバッグ情報のみを出力します。

例

#現在の端末にデバッグ情報を出力できるようにする。

<AC> terminal debugging

```
The current terminal is enabled to display debugging logs.
```

関連コマンド

- **terminal logging level**
- **terminal monitor**

5.1.30 terminal logging level

Syntax

terminal logging level *severity*

undo terminal logging level

デフォルト

現在の端末で出力が許可されているログ情報の最低レベルは 6 (Informational)です。

View

User view

定義済みユーザロール

network-admin

パラメータ

severity:0~7 の整数または alert、critical、debugging、emergency、error、informational、notification、warning の値のログ情報を出力できる現在の端末の最小レベル。

説明

terminal logging level コマンドを使用して、現在のエンドポイントが出力できるログ情報の最小レベルを設定します。

undo terminal logging level コマンドを使用して、デフォルトの状態を復元します。

現在の端末が出力可能なログ情報の最低レベルを設定した後、システムが情報を出力する際に、設定レベル以上のすべての情報レベルが出力される。例えば、ログ情報の出力を許可する最低レベル 6 (informational)が設定されている場合、レベル 0～6 の情報が出力される。

このコマンドで設定された表示属性は、現在の接続でのみ有効です。端末とデバイスの接続がタイムアウトし、接続が再確立されると、表示属性はデフォルトに戻ります。

例

デバッグレベル以上のログを現在の端末に出力するように設定します。

<AC> terminal logging level 7

5.1.31 terminal monitor

Syntax

terminal monitor

undo terminal monitor

デフォルト

コンソールへのログ情報の出力を許可し、監視端末へのログ情報の出力を許可しない。

View

User view

定義済みユーザロール

network-admin

説明

terminal monitor コマンドは、ログ情報を現在の端末に出力できるようにするために使用します。

undo terminal monitor コマンドは、ログ情報が現在の端末に出力されないようにするために使用します。

このコマンドは、現在の接続に対してのみ有効です。端末がデバイスに再接続すると、このコマンドはデフォルトに戻ります。

例

#ログ情報を現在のエンドポイントに出力することを許可します。

<AC> terminal monitor

```
The current terminal is enabled to display logs.
```

5.1.32 timestamp

Syntax

timestamp { **date** [**with-milliseconds**] | **iso** [**with-milliseconds** | **with-timezone**] * | **no-year-date** | **none** }

undo timestamp

デフォルト

ログのタイムスタンプの形式は date です。

View

Log output profile view

定義済みユーザロール

network-admin

パラメータ

date:タイムスタンプ形式を MMM DD hh:mm:ss YYYY に設定します (例:12 月 8 日 10:12:21 2019) 。日付時刻は現在のシステム時刻を示します。

with-milliseconds:日付または ISO 8601 形式でログホストに出力されるログのタイムスタンプを正確にミリ秒に設定します。ミリ秒の値は、ドットを区切り文字としてタイムスタンプ内の時刻情報に付加されます。このキーワードを指定しない場合、日付または ISO 8601 形式のタイムスタンプは秒単位で正確です。

- ミリ秒の精度を持つ日付形式のタイムスタンプの例:12 月 8 日 10:12:21.708 2019。
- ISO 8601 形式でミリ秒単位の精度を持つタイムスタンプの例:2019-09-21 T 15:32:55.708。

iso:ISO 8601 タイムスタンプ形式を設定します (例:2019-09-21 T 15:32:55) 。

with-timezone:タイムゾーン情報を ISO 形式のタイムスタンプに含めます。例:2019-09-21 T 15:32:55+01:00。デフォルトでは、ISO 形式のタイムスタンプにタイムゾーン情報は含まれません。

no-year-date:タイムスタンプ形式を、年やミリ秒の情報を含まない現在のシステム日時に設定します。

none:タイムスタンプ情報が提供されないことを示します。

説明

ログのタイムスタンプ形式を設定するには、**timestamp** を使用します。

デフォルトに戻すには、**undo timestamp** を使用します。

例

#ログ出力プロファイル profile 1 を作成し、ログのタイムスタンプ形式を no-year-date に設定する。

<AC> system-view
[AC] info-center output-profile profile1
[AC-ic-profile-profile1] timestamp no-year-date

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

4. インタフェース

本マニュアルは以下に示す章で構成されています。

01-インタフェース共通

02- ループバックインタフェースと Null インタフェース

03- Ethernet インタフェース

04- Interface range

目次

このセクションのページは **4-x-x** です。

1 章 インタフェース共通 1-1
1.1 インタフェース共通コマンド 1-1
1.1.1 description 1-1
1.1.2 display counters 1-1
1.1.3 display counters rate 1-3
1.1.4 display interface main 1-5
1.1.5 reset counters interface 1-20
1.1.6 shutdown 1-21

1章 インタフェース共通

1.1 インタフェース共通コマンド

1.1.1 description

Syntax

description *text*

undo description

デフォルト

インタフェースの説明情報は、GigabitEthernet1/0/1 Interface のように「インタフェース名 Interface」です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

text:インタフェースの説明情報。1~255 文字の文字列で、大文字と小文字が区別されます。

説明

description コマンドは、現在のインタフェースの説明情報を設定します。

undo description コマンドを使用して、デフォルトの状態を復元します。

例

#設定インタフェース GigabitEthernet1/0/1 の説明情報は「lan-interface」です。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] description lan-interface

1.1.2 display counters

Syntax

display counters { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound:入力メッセージのトラフィック統計情報を表示します。

outbound:出力メッセージのトラフィック統計情報を表示します。

interface-type:インタフェースのタイプを指定します。

interface-number:インタフェース番号を指定します。

説明

display counters コマンドを使用して、インタフェースのトラフィック統計情報を表示します。

インタフェースの統計情報は、**reset counters interface** コマンドでクリアできます。

インタフェースタイプを指定しない場合は、すべての統計可能なインタフェースのトラフィック統計情報が表示されます。

インタフェース番号を指定せずにインタフェースタイプを指定すると、そのタイプのすべてのインタフェースのトラフィック統計情報が表示されます。

インタフェースタイプとインタフェース番号の両方を指定すると、指定したインタフェース/サブインタフェースのメッセージトラフィック統計情報が表示されます。

例

#インタフェースのメッセージ入力トラフィックの統計情報を表示します。

<Sysname> display counters inbound interface

Interface	Total (pkts)	Broadcast (pkts)	Multicast (pkts)	Err (pkts)
GE1/0/1	100	100	0	0
GE1/0/2	Overflow	Overflow	Overflow	Overflow

Overflow: More than 14 digits (7 digits for column "Err").

--: Not supported.

表1-1 display counters コマンドの表示情報の説明

フィールド	説明
Interface	インタフェース名の省略名
Total (pkts)	インタフェースで受信または送信されたメッセージの合計数(単位はパッケージ)

フィールド	説明
Broadcast (pkts)	インタフェースがブロードキャストメッセージを受信または送信した合計数(単位はパッケージ)
Multicast (pkts)	インタフェースで受信または送信されたマルチキャストメッセージの総数(単位はパッケージ)
Err (pkts)	インタフェースが受信または送信したエラーメッセージの合計数(単位はパッケージ)
Overflow:More than 14 digits (7 digits for column "Err").	統計の値がOverflowの場合は、データの長さが表示範囲を超えています。 • Err 項の場合、Overflow はデータの長さが 7 桁の 10 進数を超えていることを示します。 • その他のアイテムの場合、Overflow は、データの長さが 14 桁の 10 進数を超えていることを示します。
--: Not supported.	統計の値が「--」の場合は、デバイスがその統計をサポートしていないことを示します。

関連コマンド

- **reset counters interface**

1.1.3 display counters rate

Syntax

display counters rate { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound:メッセージ受信レートの統計情報を表示します。

outbound:メッセージ送信レートの統計情報を表示します。

interface-type:インタフェースのタイプを指定します。

interface-number:インタフェース番号を指定します。

説明

display counters rate コマンドを使用して、最後の統計期間に up 状態だったインタフェースのメッセージレート統計情報を表示します。

interface-type と interface-number を指定しない場合は、すべての統計情報可能なインタフェースタイプのうち、最後の統計期間に up 状態だったインタフェースのメッセージレート統計情報が表示されます。

interface-type を指定し、interface-number を指定しない場合は、このタイプの最後の統計期間中に up 状態だったインタフェースのメッセージレート統計情報が表示されます。

interface-type と interface-number の両方を指定すると、指定したインタフェースの最新の統計期間中のメッセージレート統計情報が表示されます。最後の統計期間中にインタフェースがダウンしていた場合は、インタフェースがこの操作をサポートしていないことが通知されます。

統計期間は、**flow-interval** コマンドを使用して設定できます。

例

#インタフェースのメッセージ受信レート統計情報を表示します。

<Sysname> display counters rate inbound interface

Usage: Bandwidth utilization in percentage

Interface	Usage (%)	Total (pps)	Broadcast (pps)	Multicast (pps)
GE1/0/1	0	0	--	--

Overflow: More than 14 digits.

--: Not supported.

表1-2 display counters rate コマンドの表示情報の説明

フィールド	説明
Interface	インタフェース名の省略名
Usage (%)	直近の統計期間におけるインタフェースの帯域幅使用率(単位:パーセント)
Total (pps)	最近の統計期間中にインタフェースがすべてのタイプのメッセージを送受信した平均レート(単位はパケット/秒)
Broadcast (pps)	最近の統計期間中にインタフェースがブロードキャストメッセージを受信または送信した平均レート(単位はパケット/秒)
Multicast (pps)	最近の統計期間中にインタフェースがマルチキャストメッセージを受信または送信した平均レート(単位はパケット/秒)
Overflow:More than 14 digits.	統計の値がOverflowの場合、データの長さが14桁の10進数を超えています。
--: Not supported.	統計の値が「--」の場合は、デバイスがその統計をサポートしていないことを示します。

関連コマンド

- flow-interval (インタフェース-Ethernet インタフェース)
- reset counters interface

1.1.4 display interface main

Syntax

display interface [*interface-type*] [**brief** [**description** | **down**]] **main**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type:インタフェースのタイプを指定します。このパラメータを指定しない場合は、すべてのタイプのインタフェースの情報が表示されます。

brief:インタフェースのサマリー情報を表示します。このパラメータを指定しないと、インタフェースの詳細が表示されます。

description:ユーザが設定したインタフェースのすべての説明情報を表示します。あるインタフェースの記述情報が 27 文字を超える場合、このパラメータを指定しないと記述情報の最初の 27 文字しか表示されず、それを超える部分は表示されない。

down:現在の物理状態が down であるインタフェースの情報と down の理由を表示します。このパラメータを指定しない場合、インタフェースの物理状態に基づいて表示情報がフィルタリングされません。

説明

display interface main コマンドを使用して、サブインタフェース以外のインタフェースの動作ステータスと関連情報を表示します。

例

#サブインタフェース以外のインタフェースの動作ステータスと関連情報を表示します。

<Sysname> display interface main

GigabitEthernet1/0/1

Current state: Administratively DOWN

Line protocol state: DOWN

IP packet frame type: Ethernet II, hardware address: 4005-6538-0100

Description: GigabitEthernet1/0/1 Interface

Bandwidth: 1000000 kbps
Loopback is not set
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: Automdix
Port link-type: Access
 Tagged VLANs: None
 Untagged VLANs: 1
Port priority: 2
Last link flapping: Never
Last clearing of counters: Never
Current system time:2018-04-11 10:20:24
Last time when physical state changed to up:-
Last time when physical state changed to down:2018-04-11 09:11:09
 Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
 Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
 Last 300 seconds input: 0 packets/sec 0 bytes/sec -%
 Last 300 seconds output: 0 packets/sec 0 bytes/sec -%
 Input (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input (normal): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Input: 0 input errors, 0 runts, 0 giants, 0 throttles
         0 CRC, 0 frame, 0 overruns, 0 aborts
         0 ignored, 0 parity errors
 Output (total): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output (normal): 0 packets, 0 bytes
         0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
 Output: 0 output errors, 0 underruns, 0 buffer failures
         0 aborts, 0 deferred, 0 collisions, 0 late collisions
         0 lost carrier, 0 no carrier
IPv4 traffic statistics:
 Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec
 Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec
 Input: 0 packets, 0 bytes

```
  Output: 0 packets, 0 bytes
IPv6 traffic statistics:
  Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec
  Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec
  Input: 0 packets, 0 bytes
  Output: 0 packets, 0 bytes

GigabitEthernet1/0/2
Current state: Administratively DOWN
Line protocol state: DOWN
Description: GigabitEthernet1/0/2 Interface
Bandwidth: 1000000 kbps
Flow-control is not enabled
Maximum transmission unit: 1500
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 4005-6538-0107
IPv6 packet frame type: Ethernet II, hardware address: 4005-6538-0107
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: Never
Last clearing of counters: Never
Current system time:2018-04-11 10:20:24
Last time when physical state changed to up:-
Last time when physical state changed to down:2018-04-11 09:33:52
  Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
  Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
  Last 300 seconds input: 0 packets/sec 0 bytes/sec -%
  Last 300 seconds output: 0 packets/sec 0 bytes/sec -%
  Input (total):    0 packets, 0 bytes
                0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
  Input (normal):    0 packets, 0 bytes
                0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
  Input:    0 input errors, 0 runts, 0 giants, 0 throttles
                0 CRC, 0 frame, 0 overruns, 0 aborts
                0 ignored, 0 parity errors
  Output (total): 0 packets, 0 bytes
                0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
  Output (normal): 0 packets, 0 bytes
```

```
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
  Output: 0 output errors, 0 underruns, 0 buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        0 lost carrier, 0 no carrier
IPv4 traffic statistics:
  Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec
  Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec
  Input: 0 packets, 0 bytes
  Output: 0 packets, 0 bytes
IPv6 traffic statistics:
  Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec
  Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec
  Input: 0 packets, 0 bytes
  Output: 0 packets, 0 bytes
```

表1-3　display interface main コマンドの表示情報の説明

フィールド	説明
GigabitEthernet1/0/1	インタフェースGigabitEthernet1/0/1に関する情報
Current state	インタフェースの物理状態。状態は次のとおりです。 • Administratively DOWN:インタフェースが shutdown コマンドでシャットダウンされたことを示します。つまり、管理状態はシャットダウンです。 • DOWN:このインタフェースの管理ステータスが ON で、物理ステータスが OFF であることを示します(物理的な接続がないか、回線が故障している可能性があります) • DOWN (Link-Aggregation interface down):このインタフェースが属する集約インタフェースが shutdown コマンドによってシャットダウンされたことを示します。 • Link-Flap DOWN:インタフェースがリンクフラップ保護機能によってシャットダウンされていることを示します。 • mac-address moving down:MAC アドレスの移行抑制によるインタフェースのシャットダウン • Storm-Constrain:不明なユニキャスト、マルチキャスト、またはブロードキャストメッセージのトラフィックが上限しきい値を超えたため、ポートでシャットダウンされたことを示します。 • STP DOWN:STP BPDU 保護がトリガーされたためにインタフェースが自動的にシャットダウンされたことを示します • UP:このポートの管理状態と物理状態の両方がオンです。

フィールド	説明
Line protocol state	インタフェースのリンク層プロトコルステータス。この値は、パラメータのネゴシエーションを経てリンク層によって決定され、以下の値をとります。 • UP:データリンク層プロトコルのステータスがオンであることを示します。 • UP (spoofing):インタフェースのデータリンク層プロトコルステータスがオンであるが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があることを示します。通常、NULL、LoopBack などのインタフェースにはこの属性があります。 • DOWN:データリンク層プロトコルのステータスがオフであることを示します。 • DOWN (protocols):インタフェースのデータリンク層が 1 つ以上のプロトコルモジュールによってシャットダウンされたことを示します。protocols は LAGG です。 　o LAGG:集約インタフェースのメンバーポートが選択されていないためにインタフェースがダウンしているデータリンク層を示します
Description	インタフェースの説明
Bandwidth	インタフェースの予想帯域幅
Maximum transmission unit	インタフェースのMTU
Internet protocol processing	インタフェースにIPアドレスが設定されていない場合、インタフェースのネットワークプロトコル設定パラメータ: • Disabled:IP メッセージを処理できません • Enabled:IP メッセージを処理できます。

フィールド	説明
Internet address:ip-address/mask-length (Type)	インタフェースのIPアドレス。Typeはアドレスの取得方法を示し、値は次のとおりです。 • Primary:手動で構成されたプライマリ・アドレス • Sub:手動で設定されたスレーブアドレス。プライマリ・アドレスが構成されている場合は、プライマリ・アドレスのみが表示されます。この情報は、スレーブアドレスが設定されている場合にのみ表示されます。 • DHCP-allocated:DHCP で取得した IP アドレス。 • BOOTP-allocated:BOOTP で取得した IP アドレス。 • Unnumbered:別のインタフェースの IP アドレスを借用します DHCP の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“5 ネットワーク接続”の”DHCP”を参照してください（DHCP 関連は 12 章から 17 章に記載しています）。
IP packet frame type	IPv 4メッセージ送信フレームフォーマット
hardware address	インタフェースのMACアドレス
IPv6 packet frame type	IPv 6メッセージ送信フレームフォーマット
Media type is	インタフェースのメディアタイプ
Port hardware type is	インタフェースのハードウェアタイプ
Port priority	インタフェースプライオリティ
Loopback is set internal	イーサネットインタフェースの内部ループバックテストが実行されています。ユーザの設定に関連する情報が表示されます。
Loopback is set external	イーサネットインタフェースの外部ループバックテストを実行します。このテストは、ユーザの構成に関係します。
Loopback is not set	ループバックテストがインタフェースで設定されていません。ユーザの設定に関連する情報が表示されます。
100 Mbps-speed mode	インタフェース速度は100 Mbpsで、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。
1000 Mbps-speed mode	インタフェース速度は1000 Mbpsで、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。
10 Gbps-speed mode	インタフェース速度は10 Gbpsで、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。
Unknown-speed mode	レートネゴシエーションに失敗したか、インタフェースが物理的に接続されていないため、レートは不明です。
half-duplex mode	インタフェースは半二重モードで動作し、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。

フィールド	説明
full-duplex mode	インタフェースは全二重モードで動作し、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。
unknown-duplex mode	デュアルモードネゴシエーションが失敗したか、インタフェースが物理的に接続されていないため、不明なデュアルモード
Link speed type is autonegotiation	ユーザがspeed autoを設定した場合に表示されます。
Link speed type is force link	この情報は、ユーザがspeedコマンドを使用して特定のレートを設定した場合に表示されます。たとえば、1000 Mなどです。
link duplex type is autonegotiation	ユーザがduplex autoを設定した場合に表示されます。
link duplex type is force link	この情報は、duplexコマンドを使用してhalfやfullなどの特定のデュプレックスモードが設定されている場合に表示されます。
Flow-control is not enabled	フロー制御機能が設定されていません。この表示情報は、ユーザの設定およびリンクパラメータのネゴシエーション結果に関連しています。
Maximum frame length	インタフェースが通過できるイーサネットフレームの最大長
Allow jumbo frame to pass	長いフレームの通過を許可
Broadcast max-	ブロードキャストストーム抑制しきい値は、ユーザの設定に応じて、ratio (パーセント)、pps、またはkbpsのいずれかになります。
Multicast max-	ユーザの設定に関連するマルチキャストストーム抑制しきい値は、ratio (パーセント)、pps、またはkbpsのいずれかです。
Unicast max-	不明なユニキャストストーム抑制しきい値。ユーザの設定に応じて、ratio (パーセント)、pps、またはkbpsのいずれかになります。
PVID	インタフェースが存在するデフォルトVLAN ID
MDI type	ユーザの構成に関連するautomdix、mdi、またはmdixの値を持つネットワークケーブルのタイプ
Port link-type	ユーザの構成に応じて、access、trunk、またはhybridの値を持つリンクタイプ
Tagged VLANs	このインタフェースを介してTagを持つVLAN
UnTagged VLANs	このインタフェースを通過した後にTagを持たないVLAN
VLAN Passing	インタフェースが実際に通過できるVLAN (インタフェースで許可され、作成されたVLAN)
VLAN permitted	インタフェースで許可されているVLANメッセージ
Trunk port encapsulation	Trunkインタフェースのカプセル化形式
Last link flapping	インタフェースの物理状態が最後に変更されてからの経過時間。Neverは、インタフェースがデバイスの起動時からダウンしていることを示します(変わったことはありません)。

フィールド	説明
Last clearing of counters	最後にreset counters interfaceコマンドを使用してインタフェースの統計情報をクリアした時刻(デバイスからの起動時にreset counters interfaceコマンドを実行せずにインタフェースの統計情報をクリアした場合は、Neverと表示されます。)
Current system time	現在のシステム時刻、時刻はYYYY/MM/DD HH:MM:SSの形式で表示されます。 タイムゾーンが構成されている場合は、現在のシステム時刻の後にタイムゾーンを表示する構成がYYYY/MM/DD HH:MM:SS zone-name± HH:MM:SSの形式で追加されます。ここで、zone-nameはローカル・タイムゾーン名です。
Last time when physical state changed to up	最後にインタフェースの物理ステータスがUPになった時刻 タイムゾーンが構成されている場合は、タイムゾーンの構成がYYYY/MM/DD HH:MM:SS zone-name±HH:MM:SSの形式で追加されます。ここで、zone-nameはローカル・タイムゾーン名です。 「-」 は、インタフェースの物理的な状態が変化していないことを示します。
Last time when physical state changed to down	最後にインタフェースの物理状態がDOWNになった時刻 タイムゾーンが構成されている場合は、タイムゾーンの構成がYYYY/MM/DD HH:MM:SS zone-name±HH:MM:SSの形式で追加されます。ここで、zone-nameはローカル・タイムゾーン名です。 「-」 は、インタフェースの物理的な状態が変化していないことを示します。
Last 300 seconds input:0 packets/sec 0 bytes/sec 0% Last 300 seconds output:0 packets/sec 0 bytes/sec 0%	過去300秒間にポートがパケット/秒およびバイト/秒の単位でメッセージを送受信した平均レート、および実際のレートとインタフェース帯域幅の割合 値が 「-」 の場合、統計はサポートされていません
Input (total):0 packets、0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	ポートが受信したメッセージの統計値。通常のメッセージ、例外メッセージ、通常のPAUSEフレームのメッセージ数、バイト数を含む。 ポートが受信するユニキャスト、ブロードキャスト、マルチキャスト、およびPAUSEフレームの数 値が 「-」 の場合、統計はサポートされていません
Input (normal):0 packets、0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	ポートが受信した通常のメッセージの統計値。通常のメッセージと通常のPAUSEフレームのメッセージ数、バイト数を含む。 ポートが受信する通常のユニキャスト、ブロードキャスト、マルチキャスト、およびPAUSEフレームの数 値が 「-」 の場合、統計はサポートされていません

フィールド	説明
input errors	ポートが受信したエラーメッセージの統計値
runts	受信した超小フレームの数 超小フレームとは、64バイト未満で、正しい形式で、有効なCRCフィールドを含むフレームです。
giants	受信したジャンボフレームの数 ジャンボフレームは、ポートが許可する最大メッセージ長よりも長い有効長を持つフレームです。 • 長いフレームが通過できないイーサネットポートの場合、ジャンボフレームとは、有効長が 1518 バイト(なし VLAN Tag)を超えるフレーム、または 1522 バイト(VLAN Tag メッセージ付き)を超えるフレームを指します。 • 長いフレームが通過できるイーサネットポートの場合、ジャンボフレームは指定された最大フレーム長より長い有効長を持つフレームです。
throttles	受信した非整数バイト長のフレームの数
CRC	受信したCRCチェックエラーの正常な長さのフレームの数
frame	受信したCRC検証エラーで、長さが整数バイトではないフレームの数
overruns	ポートの受信レートが受信キューの処理能力を超えると、メッセージがドロップされる

フィールド	説明
aborts	受信した不正メッセージの総数。不正メッセージには次のものが含まれます。 • メッセージフラグメント:長さが 64 バイト未満(長さは整数または整数以外のいずれかです。)で、CRC チェックエラーのあるフレーム • jabber フレーム:有効長がポートが通過できる最大メッセージ長より長く、CRC チェックが正しくないフレーム(長さは、整数バイトまたは非整数バイトのいずれかです。)。長いフレームの通過が禁止されているイーサネットポートの場合、jabber フレームは、1518 (なし VLAN Tag)または 1522 (帯 VLAN Tag)バイトを超える CRC チェックエラーのあるフレームです。長いフレームが通過できるイーサネットポートの場合、jabber フレームは、指定された最大フレーム長よりも長い有効長を持ち、CRC チェックエラーが発生したフレームです。 • シンボルエラーフレーム:メッセージに少なくとも 1 つのエラーが含まれているシンボル • オペコード不明フレーム:メッセージは MAC 制御フレームですが、Pause フレームではありません。 • 長さエラーフレーム:メッセージの長さフィールド 802.3 がメッセージの実際の長さ(46~1500 バイト)と一致しません。
ignored	ポートの受信バッファ不足などによりドロップされたメッセージ数
parity errors	受信したパリティエラーのフレーム数
Output (total):0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	ポートが送信するメッセージの統計値。通常のメッセージ、例外メッセージ、通常のPAUSEフレームのメッセージ数、バイト数を含む。 ポートから送信されるユニキャスト、ブロードキャスト、マルチキャスト、およびPAUSEフレームの数 値が 「-」 の場合、統計はサポートされていません
Output (normal):0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	ポートから送信された通常のメッセージの統計値。通常のメッセージと通常のPAUSEフレームのメッセージ数、バイト数を含む。 ポートから送信される通常のユニキャストメッセージ、ブロードキャストメッセージ、マルチキャストメッセージ、およびPAUSEフレームの数 値が 「-」 の場合、統計はサポートされていません
output errors	各種送信エラーのメッセージ総数
underruns	ポートの送信レートが送信キューの処理能力を超え、メッセージがドロップされることは、非常にまれなハードウェア例外です。
buffer failures	ポート送信バッファが不足しているためにドロップされたメッセージの数

フィールド	説明
aborts	送信に失敗したメッセージの合計数、つまりメッセージの送信が開始されたが、さまざまな理由(例えば)により送信に失敗したメッセージの数
deferred	遅延メッセージの数、遅延メッセージとは送信前に衝突を検出して遅延送信されたメッセージである.
collisions	衝突フレーム数、衝突フレームとは送信中に衝突を検出し、送信を停止したメッセージである.
late collisions	フレームの最初の512 bitsが送信され、衝突が検出されたために送信が遅延された遅延衝突フレームの数
lost carrier	搬送波損失、一般的にシリアルWANインタフェースに適用、送信中に1つの搬送波損失ごとにこのカウンタに加算
no carrier	キャリアなし、一般的にシリアルWANインタフェースに適用されます。フレームを送信しようとしたときにキャリアが表示されない場合は、このカウンタに1が加算されます。
Peak input rate	インタフェースの入力トラフィックのピークレートのサイズ(単位はbytes/secです)とピークが発生した時間
Peak output rate	インタフェース出力トラフィックのピークレートのサイズ(単位はbytes/secです)とピークが発生した時間
IPv4 traffic statistics	IPv 4メッセージ統計
IPv6 traffic statistics	IPv 6メッセージ統計
Last 300 seconds input rate:0 packets/sec, 0 bytes/sec	過去300秒間にポートがパケット/秒とバイト/秒でメッセージを送受信した平均レート 値が 「-」 の場合、統計はサポートされていません
Last 300 seconds output rate:0 packets/sec, 0 bytes/sec	過去300秒間にポートが送信したパケット/秒とバイト/秒の平均レート 値が 「-」 の場合、統計はサポートされていません
Input:0 packets, 0 bytes	ポートが受信したメッセージの統計値。メッセージ数、バイト数を含む。 値が 「-」 の場合、統計はサポートされていません
Output:0 packets, 0 bytes	ポートが送信するメッセージの統計値。メッセージ数、バイト数を含む。 値が 「-」 の場合、統計はサポートされていません

#サブインタフェース以外のすべてのインタフェースのサマリー情報を表示します。

<Sysname> display interface brief main

Brief information on interfaces in route mode:

Link: ADM - administratively down; Stby - standby

Protocol: (s) – spoofing

```
Interface                Link Protocol Primary IP          Description
GE1/0/1                  DOWN DOWN       --
Loop0                    UP   UP(s)      2.2.2.9
NULL0                    UP   UP(s)      --
Vlan1                    UP   DOWN       --
Vlan999                  UP   UP         192.168.1.42

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface                Link Speed   Duplex Type PVID Description
GE1/0/2                  DOWN auto    A      A    1
```

#サブインタフェース以外のインタフェースの概要情報を表示します。この情報には、ユーザ設定のすべての説明が含まれます。

<Sysname> display interfacebrief description main

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface                Link Speed   Duplex Type PVID Description
GE1/0/3                  UP   auto    F(a)   A    1    aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

#サブインタフェース以外の現在の物理状態が down のインタフェースの情報と down の理由を表示します。

<Sysname> display interface brief down main

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface                Link Cause
GE1/0/1                  DOWN Not connected
Vlan2                    DOWN Not connected

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface                Link Cause
GE1/0/2                  DOWN Not connected
```

表1-4 display interface brief main コマンドの表示情報の説明

フィールド	説明
Brief information on interfaces in route mode:	3層モード(route)のインタフェースのサマリー情報、つまり3層インタフェースのサマリー情報
Link: ADM - administratively down; Stby - standby	• インタフェースの Link プロパティの値が「ADM」の場合、そのインタフェースは、shutdown コマンドを使用して管理者によってシャットダウンされました。インタフェース自体の物理状態を復元するには、そのインタフェースで undo shutdown コマンドを実行する必要があります。 • インタフェースの Link プロパティの値が「スティビー」の場合は、そのインタフェースが Standby のバックアップインタフェースであることを示します。
Protocol: (s) - spoofing	インタフェースのProtocol属性値に「(s)」が含まれている場合は、そのインタフェースのデータリンク層プロトコルステータスがUPと表示されますが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があります。通常、NULL、LoopBackなどのインタフェースにはこの属性があります。
Interface	インタフェース名の省略名
Link	インタフェースの物理接続ステータス。次の値をとります。 • UP:インタフェースが物理的に接続されていることを示します。 • DOWN:インタフェースが物理的に機能していないことを示します。 • ADM:管理者が shutdown コマンドを使用してインタフェースをシャットダウンしたことを示します。インタフェース自体の物理状態を回復するには、undo shutdown コマンドを実行する必要があります。 • Stby:インタフェースが状態 Standby のバックアップインタフェースであることを示します。

フィールド	説明
Protocol	インタフェースデータリンク層プロトコルの状態。次の値を取ります。 • UP:インタフェースのデータリンク層プロトコルステータスがオンであることを示します。 • DOWN:インタフェースのデータリンク層プロトコルの状態がオフであることを示します • [UP (s)] :インタフェースのデータリンク層プロトコルステータスが [UP] と表示されているが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があります。通常、NULL、LoopBack などのインタフェースはこの値を取ります。
Primary IP	インタフェースのプライマリIPアドレス。値が「--」の場合は、インタフェースにIPアドレスが設定されていません。
Description	インタフェースの説明
Brief information of interfaces in bridge mode:	2層モード(bridge)のインタフェース・サマリー情報、つまり2層インタフェースのサマリー情報
Speed: (a) -auto	インタフェースのSpeedプロパティの値が「(a)」の場合、インタフェースのレートはオートネゴシエーションによって取得されます。インタフェースのSpeedプロパティの値が「auto」の場合、そのインタフェースのレートは自動ネゴシエーションによって取得されますが、ネゴシエーションはまだ開始されていません。
Duplex: (a) /A - auto;H - half;F - full	インタフェースのDuplex属性の値が「(a)」または 「A」 の場合、そのインタフェースのDuplex属性は自動ネゴシエーションによって取得されます。半二重の場合は 「H」;「F」 を指定すると全二重になります。 「A」 と表示されている場合は、インタフェースのDuplex属性が自動ネゴシエーションによって取得されたが、ネゴシエーションが開始されていないことを示します。
Type:A - access;T - trunk;H - hybrid	インタフェースのリンクタイプ: • A:Access リンクタイプを示します。 • H:Hybrid リンクタイプを示します。 • T:Trunk リンクタイプを示します。
Speed	インタフェースのビット/秒単位のレート

フィールド	説明
Duplex	インタフェースのデュプレックスモード。値は次のとおりです。 • A:デュプレックスモードがオートネゴシエーションの結果によって決定されることを示します。 • F:全二重を表します。 • F (a) :自由ネゴシエーションの結果が全二重であることを示す. • H:半二重 • H (a) :自由ネゴシエーションの結果が半二重であることを示す.
Type	インタフェースのリンクタイプ: • A:Access リンクタイプを示します。 • H:Hybrid リンクタイプを示します。 • T:Trunk リンクタイプを示します。
PVID	インタフェースが存在するデフォルトVLAN ID
Cause	インタフェースの物理接続ステータスがdownである理由は、次のとおりです。 • Administratively:このリンクが手動でダウンしたことを示します(shutdown コマンドが設定されました)。実際の物理状態に戻すには、undo shutdown コマンドを実行する必要があります。 • DOWN (Link-Aggregation interface down):集約インタフェースがダウンすると、その集約インタフェースのすべてのメンバーポートのステータスが DOWN と表示され、ダウンの理由が DOWN (Link-Aggregation interface down)と表示されます。 • DOWN (Loopback detection down):ループ検出モジュールがループを検出したため、インタフェースが自動的にシャットダウンされました • Not connected:物理的な接続がないことを示します(ネットワークケーブルが接続されていないか、ネットワークケーブルに問題がある可能性があります。)。 • Storm-Constrain:不明なユニキャスト、マルチキャスト、またはブロードキャストメッセージのトラフィックが上限しきい値を超えたため、ポートでシャットダウンされたことを示します。 • STP DOWN:STP BPDU 保護がトリガーされたためにインタフェースが自動的にシャットダウンされました • Standby:インタフェースがバックアップ状態であることを示します。

1.1.5 reset counters interface

Syntax

reset counters interface [*interface-type* [*interface-number* | *interface-number.subnumber*]]

View

ユーザビュー

定義済みユーザロール

network-admin

パラメータ

interface-type:インタフェースのタイプを指定します。

interface-number:インタフェース番号を指定します。

interface-number.subnumber:サブインタフェースを指定します。ここで、interface-number はプライマリインタフェース番号です。subnumber はサブインタフェース番号で、値の範囲は 1~4094 です。

説明

reset counters interface コマンドは、インタフェースの統計情報をクリアするために使用されます。

場合によっては、ある一定時間内のあるインタフェースのトラヒックをカウントする必要があるため、カウントを開始する前にそのインタフェースの既存の統計情報を消去し、再度カウントする必要がある。

interface-type と interface-number を指定しない場合は、すべてのインタフェースの統計情報がクリアされます。

interface-number ではなく interface-type を指定すると、そのタイプのすべてのインタフェースの統計情報がクリアされます。

例

#イーサネットインタフェース GigabitEthernet1/0/1 の統計情報をクリアします。

<Sysname> reset counters interface gigabitethernet 1/0/1

関連コマンド

- **display interface**
- **display counters interface**
- **display counters rate interface**

1.1.6 shutdown

Syntax

shutdown

undo shutdown

デフォルト

イーサネットインタフェースはオンです。

View

Interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドは、インタフェースをシャットダウンするために使用されます。

undo shutdown コマンドは、インタフェースを開くために使用されます。

 注意

このコマンドを実行すると、そのインタフェースを使用して確立されたリンクが切断され、通信できなくなる可能性があります。注意して使用してください。

特定の状況(たとえば、インタフェースの作業パラメータの変更)では、インタフェース関連の設定はすぐには有効にならず、インタフェースをシャットダウンして再び開く必要があります。

例

#インタフェース GigabitEthernet1/0/1 を閉じた後、インタフェースを開きます。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] shutdown
[Sysname-GigabitEthernet1/0/1] undo shutdown

目次

このセクションのページは **4-x-x** です。

2 章 ループバックインタフェースと Null インタフェース 2-1
2.1 ループバックインタフェースと Null インタフェースコマンド 2-1
2.1.1 display interface loopback 2-1
2.1.2 display interface null 2-6
2.1.3 interface loopback 2-7
2.1.4 interface null 2-8

2章 ループバックインタフェースと Null インタフェース

2.1 ループバックインタフェースとNullインタフェースコマンド

2.1.1 display interface loopback

Syntax

display interface [**loopback** [*interface-number*]] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

loopback *interface-number*:LoopBack 作成された LoopBack インタフェースの数の範囲を取るインタフェースの数。loopback パラメータを指定しない場合、デバイスがサポートするすべてのインタフェースに関する情報が表示されます。loopback パラメータを指定し、interface-number パラメータを指定しない場合、作成されたすべての LoopBack インタフェースに関する情報が表示されます。

brief:インタフェースのサマリー情報を表示します。このパラメータを指定しないと、インタフェースの詳細が表示されます。

description:ユーザが設定したインタフェースのすべての説明情報を表示します。あるインタフェースの記述情報が 27 文字を超える場合、このパラメータを指定しないと記述情報の最初の 27 文字しか表示されず、それを超える部分は表示されない。

down:現在の物理状態が down であるインタフェースの情報と down の理由を表示します。このパラメータを指定しない場合、インタフェースの物理状態に基づいて表示情報がフィルタリングされません。

説明

display interface loopback コマンドは、LoopBack インタフェースに関する情報を表示するために使用されます。

display interface loopback コマンドは、Loopback インタフェースに関する情報を表示するために使用されます。このコマンドは、LoopBack インタフェースが作成されている場合にのみサポートされます。

例

#LoopBack0 インタフェースに関する情報を表示します。

<Sysname> display interface loopback 0

LoopBack0

Current state:UP

Line protocol state:UP (spoofing)

Description:LoopBack0 Interface

Bandwidth:1000 kbps

Maximum transmission unit:1536

Internet protocol processing:Disabled

Physical:Loopback

Last clearing of counters:Never

Last 300 seconds input rate:0 bytes/sec, 0 bits/sec, 0 packets/sec

Last 300 seconds output rate:0 bytes/sec, 0 bits/sec, 0 packets/sec

Input:0 packets, 0 bytes, 0 drops

Output:0 packets, 0 bytes, 0 drops

表 2-1　display interface loopback コマンドの表示情報の説明

フィールド	説明
Current state	インタフェースの現在の物理層状態 • UP:インタフェースがメッセージを送受信できることを示す • Administratively DOWN:インタフェースが手動でシャットダウンされたことを示します。つまり、インタフェースに shutdown コマンドが設定されています。
Line protocol state	Link Layer Protocol Status:UP (spoofing)は、インタフェースのLink Layer Protocol StatusがUPであるが、実際には対応するリンクが存在しないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があることを示します。
Description	インタフェースの説明
Bandwidth	0時以外の値を指定した場合にのみ表示されるインタフェースの予想帯域幅
Maximum transmission unit	インタフェースのMTU

フィールド	説明
Internet protocol processing	インタフェースにIPアドレスが設定されていない場合、インタフェースのネットワークプロトコル設定パラメータ: • Disabled:IP メッセージを処理できません • Enabled:IP メッセージを処理できます。
Internet address:ip-address/mask-length (Type)	インタフェースのIPアドレス。Typeはアドレスの取得方法を示し、値は次のとおりです。 • Primary:手動で構成されたプライマリ・アドレス • Sub:手動で設定されたスレーブアドレス。プライマリ・アドレスが構成されている場合は、プライマリ・アドレスのみが表示されます。この情報は、スレーブアドレスが設定されている場合にのみ表示されます。 • DHCP-allocated:DHCP で取得した IP アドレス。 • BOOTP-allocated:BOOTP で取得した IP アドレス。 • Unnumbered:別のインタフェースの IP アドレスを借用します DHCP の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“5 ネットワーク接続”の”DHCP”を参照してください（DHCP 関連は 12 章から 17 章に記載しています）。
Physical:Loopback	インタフェースの物理タイプはLoopbackです。
Last clearing of counters	最後にreset counters interfaceコマンドを使用してインタフェースの統計情報をクリアした時刻(デバイスからの起動時にreset counters interfaceコマンドを実行せずにインタフェースの統計情報をクリアした場合は、Neverと表示されます。)
Last 300 seconds input rate:0 bytes/sec, 0 bits/sec, 0 packets/sec	過去300秒間の平均入力速度(この情報は、インタフェースが統計機能をサポートしている場合にのみ表示されます。): • bytes/sec は、1 秒あたりの平均入力バイト数を表します。 • bits/sec は、1 秒あたりの平均入力ビット数を表します。 • packets/sec は、1 秒あたりに入力されたパケットの平均数です。

フィールド	説明
Last 300 seconds output rate:0 bytes/sec, 0 bits/sec, 0 packets/sec	過去300秒間の平均出力レート(この情報は、インタフェースが統計機能をサポートしている場合にのみ表示されます。): • bytes/sec は、1 秒あたりの平均出力バイト数を表します。 • bits/sec は、1 秒あたりに出力される平均ビット数を表します。 • packets/sec は、1 秒あたりに出力されるパケットの平均数を示します。
Input:0 packets, 0 bytes, 0 drops	インタフェースに入力されたメッセージ数、入力されたバイト数、入力されたメッセージでドロップされたメッセージ数(これらの情報は、インタフェースが統計機能をサポートしている場合にのみ表示されます。)
Output:0 packets, 0 bytes, 0 drops	インタフェースが出力するメッセージ数、入力バイト数、入力メッセージで破棄するメッセージ数(これらの情報は、インタフェースが統計機能をサポートしている場合にのみ表示されます。)

#LoopBack インタフェースのサマリー情報を表示します。

<Sysname> display interface loopback brief

Brief information on interfaces in route mode:

Link: ADM - administratively down; Stby - standby

Protocol: (s) - spoofing

Interface　　Link Protocol Primary IP　　Description

Loop1　　UP　UP(s)　--　　forLAN1

#現在の物理状態が down である LoopBack インタフェースの情報と down の理由を表示します。

<Sysname> display interface loopback brief down

Brief information on interfaces in route mode:

Link: ADM - administratively down; Stby - standby

Interface　　Link Cause

Loop1　　ADM　Administratively

表 2-2　display interface loopback brief コマンドの表示情報の説明

フィールド	説明
Brief information on interfaces in route mode:	LoopBackインタフェースの概要

フィールド	説明
Link:ADM - administratively down;Stby - standby	• インタフェースの Link プロパティの値が「ADM」の場合、そのインタフェースは、shutdown コマンドを使用して管理者によってシャットダウンされました。インタフェース自体の物理状態を復元するには、そのインタフェースで undo shutdown コマンドを実行する必要があります。 • インタフェースの Link プロパティの値が「Stby」の場合は、そのインタフェースが Standby のバックアップ・インタフェースであることを示します。
Protocol: (s) -spoofing	あるインタフェースのProtocol属性値に (s) が含まれている場合、そのインタフェースのデータリンク層プロトコルステータスは [UP] と表示されますが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があります。通常、NULL、LoopBackなどのインタフェースにはこの属性があります。
Interface	インタフェース名の省略名
Link	インタフェースの物理的な接続状態。次の値を取ります。 • UP:インタフェースが物理的に接続されていることを示します。 • DOWN:インタフェースが物理的に機能していないことを示します。 • ADM:管理者が shutdown コマンドを使用してインタフェースをシャットダウンしたことを示します。インタフェース自体の物理状態を回復するには、undo shutdown コマンドを実行する必要があります。 • Stby:インタフェースが状態 Standby のバックアップインタフェースであることを示します。
Protocol	インタフェースデータリンク層プロトコルステータス、UP (s) の値
Primary IP	インタフェースのプライマリIPアドレス
Description	インタフェースの説明
Cause	インタフェースの物理的な接続状態がdownである理由は、Administrativelyの値が設定されている場合、リンクが手動でダウンしたことを意味します(shutdownコマンドが設定されました)。実際の物理的な状態に戻すには、undo shutdownコマンドを実行する必要があります。

関連コマンド

- **interface loopback**
- **reset counters interface loopback**

2.1.2 display interface null

Syntax

display interface [**null** [0]] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

null *[0]*:NULL インタフェースの番号。null パラメータを指定しない場合は、デバイスがサポートするすべてのインタフェースに関する情報が表示されます。

brief:インタフェースのサマリー情報を表示します。このパラメータを指定しないと、インタフェースの詳細が表示されます。

description:ユーザが設定したインタフェースのすべての説明情報を表示します。あるインタフェースの記述情報が 27 文字を超える場合、このパラメータを指定しないと、記述情報の最初の 27 文字だけが表示され、それを超える部分は表示されない.;このパラメータを指定すると、すべての説明を表示できます。

down:現在の物理状態が down であるインタフェースの情報と down の理由を表示します。このパラメータを指定しない場合、インタフェースの物理状態に基づいて表示情報がフィルタリングされません。

説明

display interface null コマンドを使用して、NULL インタフェースに関する情報を表示します。

デバイスは 1 つの Null インタフェース Null0 しかサポートしていないため、パラメータ 0 が指定されているかどうかに関係なく、Null0 に関する情報が表示されます。

例

#指定されたインタフェース NULL0 に関する情報を表示します。

<Sysname> display interface null 0

NULL0

Current state: UP

Line protocol state: UP(spoofing)

Description: NULL0 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

#NULL インタフェースのサマリー情報を表示します。

<Sysname> display interface null 0 brief
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing

Interface	Link	Protocol	Primary IP	Description
NULL0	UP	UP(s)	--	

display interface null コマンド表示情報説明表 2-1 および表 2-2 を参照して下さい。

関連コマンド

- **interface null**
- **reset counters interface null**

2.1.3 interface loopback

Syntax

interface loopback *interface-number*

undo interface loopback *interface-number*

デフォルト

LoopBack インタフェースは存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number:LoopBack インタフェースの番号。範囲は 0~1023 です。

説明

interface loopback コマンドを使用して LoopBack インタフェースを作成し、LoopBack インタフェースビューに入ります。指定された LoopBack インタフェースがすでに存在する場合は、その LoopBack インタフェースビューに直接進みます。

undo interface loopback コマンドは、指定された LoopBack インタフェースを削除するために使用されます。

LoopBack インタフェースが作成されると、そのインタフェースを手動でシャットダウンしない限り、物理レイヤとリンクレイヤは常にアップ状態になります。そのため、LoopBack インタフェースを使用して接続を確立すると、インタフェースの物理状態によって接続が影響を受けることを回避でき、接続の信頼性が向上します。たとえば、LoopBack インタフェースを FTP 接続時のソースインタフェースとする。

例

#インタフェース LoopBack1 を作成します。

<Sysname> system-view
[Sysname] interface loopback 1
[Sysname-LoopBack1]

2.1.4 interface null

Syntax

interface null 0

デフォルト

デバイスは、ユーザが作成も削除もできない NULL インタフェース（NULL0）を 1 つだけサポートしています。

View

System view

定義済みユーザロール

network-admin

パラメータ

0:NULL インタフェースの番号。

説明

interface null コマンドが NULL インタフェースを入力するために使用するビュー。

例

#インタフェース NULL0 のビューに入ります。

<Sysname> system-view
[Sysname] interface null 0
[Sysname-NULL0]

目次

このセクションのページは **4-x-x** です。

3 章 Ethernet インタフェース 3-1
3.1 Ethernet インタフェースコマンド 3-1
3.1.1 broadcast-suppression 3-1
3.1.2 display interface 3-2
3.1.3 duplex 3-17
3.1.4 flow-interval 3-17
3.1.5 interface 3-18
3.1.6 jumboframe enable 3-19
3.1.7 loopback 3-20
3.1.8 multicast-suppression 3-21
3.1.9 port link-mode 3-22
3.1.10 speed 3-23
3.1.11 unicast-suppression 3-25

3章 Ethernet インタフェース

QX-W2300AC シリーズではインタフェース情報に GigabitEthernet1/0/17 および GigabitEthernet1/0/18 が表示されますが、サポートしていません。

3.1 Ethernetインタフェースコマンド

3.1.1 broadcast-suppression

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

broadcast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo broadcast-suppression

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio: ブロードキャスト抑制しきい値をインタフェース帯域幅のパーセンテージで設定します。この引数の値の範囲は 0 から 100 です。値が小さいほど、通過できるブロードキャストトラフィックは少なくなります。

pps *max-pps*: インタフェースが毎秒転送できるブロードキャストパケットの最大数を指定します。max-pps 引数の値の範囲 (pps 単位) は、0 から 1.4881×インタフェース帯域幅です。

kbps *max-kbps*: Ethernet インタフェースが 1 秒あたりに転送できるブロードキャストトラフィックの最大キロビット数を指定します。この引数の値の範囲 (kbps) は、0～インタフェース帯域幅です。

説明

broadcast-suppression コマンドを使用して、ブロードキャストストーム抑制を有効にし、ブロードキャスト抑制しきい値を設定します。

undo broadcast-suppression コマンドを使用して、ブロードキャストストーム抑制を無効にします。

ブロードキャストストーム抑制機能は、ブロードキャストトラフィックのサイズをインタフェース上のしきい値に制限します。インタフェース上のブロードキャストトラフィックがこのしきい値を超えると、トラフィックがこのしきい値を下回るまでシステムはパケットを破棄します。

broadcast-suppression コマンドはブロードキャストトラフィックを物理的に抑制するためにチップを使用します。

pps または **kbps** で設定された抑制しきい値は、チップでサポートされているステップの倍数に変換される場合があります。その結果、有効な抑制しきい値が設定されたものと異なる場合があります。有効な抑制しきい値を確認するには、装置のプロンプトを参照してください。

例

#ギガビットイーサネット 1/0/1 でブロードキャストストーム抑制閾値を 10000kbps に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] broadcast-suppression kbps 10000

3.1.2 display interface

Syntax

display interface [*interface-type* [*interface-number* | *interface-number.subnumber*]][**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type:インタフェースのタイプを指定します。

interface-number:インタフェース番号を指定します。

interface-number.subnumber:サブインタフェース番号を指定します。ここで、interface-number はプライマリインタフェース番号です。subnumber はサブインタフェース番号で、値の範囲は 1~4094 です。

brief:インタフェースのサマリー情報を表示します。このパラメータを指定しないと、インタフェースの詳細が表示されます。

description:ユーザが設定したインタフェースのすべての説明情報を表示します。あるインタフェースの記述情報が 27 文字を超える場合、このパラメータを指定しないと記述情報の最初の 27 文字しか表示されず、それを超える部分は表示されない。

down:現在の物理状態が down であるインタフェースの情報と down の理由を表示します。このパラメータを指定しない場合、インタフェースの物理状態に基づいて表示情報がフィルタリングされません。

説明

display interface コマンドを使用して、インタフェースの動作ステータスと関連情報を表示します。

インタフェースタイプとインタフェース番号を指定しない場合は、すべてのインタフェースの情報が表示されます。

インタフェースタイプのみを指定すると、そのタイプのすべてのインタフェースに関する情報が表示されます。

例

#レイヤ 3 イーサネットインタフェース GigabitEthernet1/0/1 の動作ステータスと関連情報を表示します。

```
<AC> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state:Administratively DOWN
Line protocol state:DOWN
Description:GigabitEthernet1/0/1 Interface
Bandwidth:1000000 kbps
Maximum transmission unit:1500
Allow jumbo frames to pass
Broadcast max-ratio:100%
Unknown-multicast max-ratio:100%
Unicast max-ratio:100%
Internet protocol processing:Disabled
IP packet frame type:Ethernet II, hardware address:3822-d666-bd0c
IPv6 packet frame type:Ethernet II, hardware address:3822-d666-bd0c
Media type is twisted pair、promiscuous mode set
Port priority:2
Unknown-speed mode、unknown-duplex mode
Link speed type is autonegotiation、link duplex type is autonegotiation
Flow-control is not enabled
```

The Maximum Frame Length is 4000
Last link flapping:6 hours 39 minutes 28 seconds
Last clearing of counters:Never
Current system time:2019-01-08 14:50:06
Last time when physical state changed to up:2019-01-08 14:49:45
Last time when physical state changed to down:2019-01-08 14:49:45
Peak input rate:0 bytes/sec, at 2013-07-07 16:07:11
Peak output rate:0 bytes/sec, at 2013-07-07 16:07:11
Last 300 seconds input:0 packets/sec 0 bytes/sec0%
Last 300 seconds output:0 packets/sec 0 bytes/sec0%
Input(total):0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts,-pauses
Input(normal):0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input:0 input errors, 0 runts, 0 giants, 0 throttles
0 CRC, 0 frame, 0 overruns,-aborts
-ignored,-parity errors
Output(total):0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts,-pauses
Output(normal):0 packets, 0 bytes
0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output:0 output errors,-underruns,-buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
-lost carrier,-no carrier

#レイヤ 2 イーサネットインタフェース GigabitEthernet1/0/1 の動作ステータスと関連情報を表示します。

<AC> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1
Current state:DOWN
Line protocol state:DOWN
IP packet frame type:Ethernet II, hardware address:000 c-2963-b767
Description:GigabitEthernet1/0/1 Interface
Bandwidth:100000 kbps
Loopback is not set
Media type is twisted pair、port hardware type is 1000_BASE_T_AN_SFP
Unknown-speed mode、unknown-duplex mode
Link speed type is autonegotiation、link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length:9216
Allow jumbo frame to pass
Broadcast max-ratio:100%
Unknown-multicast max-ratio:100%
Unicast max-ratio:100%

PVID:1

MDI type:Automdix

Port link-type:Access

Tagged VLANs:None

UnTagged VLANs:1

Port priority:2

Last link flapping:6 hours 39 minutes 25 seconds

Last clearing of counters:14:34:09 Tue 11/01/2011

Current system time:2019-01-08 14:50:06

Last time when physical state changed to up:2019-01-08 14:49:45

Last time when physical state changed to down:2019-01-08 14:49:45

Last 300 seconds input:0 packets/sec 0 bytes/sec -%

Last 300 seconds output:0 packets/sec 0 bytes/sec -%

Input (total):0 packets、0 bytes

0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses

Input (normal):0 packets、0 bytes

0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses

Input:0 input errors, 0 runts, 0 giants, 0 throttles

0 CRC, 0 frame, 0 overruns, 0 aborts

0 ignored、0 parity errors

Output (total):0 packets, 0 bytes

0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses

Output (normal):0 packets, 0 bytes

0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses

Output:0 output errors, 0 underruns, 0 buffer failures

0 aborts, 0 deferred, 0 collisions, 0 late collisions

0 lost carrier、0 no carrier

表 3-1 display interface コマンドの表示情報の説明

フィールド	説明
GigabitEthernet1/0/1	インタフェースGigabitEthernet1/0/1に関する情報

フィールド	説明
Current state	インタフェースの物理状態。状態は次のとおりです。 • Administratively DOWN:インタフェースが shutdown コマンドでシャットダウンされたことを示します。つまり、管理状態はシャットダウンです。 • DOWN:このインタフェースの管理ステータスが ON で、物理ステータスが OFF であることを示します(物理的な接続がないか、回線が故障している可能性があります) • DOWN (Link-Aggregation interface down):このインタフェースが属する集約インタフェースが shutdown コマンドによってシャットダウンされたことを示します。 • STP DOWN:STP BPDU 保護がトリガーされたためにインタフェースが自動的にシャットダウンされたことを示します • UP:このポートの管理状態と物理状態の両方がオンです。
Line protocol state	インタフェースのリンク層プロトコルステータス。この値は、パラメータのネゴシエーションを経てリンク層によって決定され、以下の値をとります。 • UP:データリンク層プロトコルのステータスがオンであることを示します。 • UP (spoofing):インタフェースのデータリンク層プロトコルステータスがオンであるが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があることを示します。通常、NULL、LoopBack などのインタフェースにはこの属性があります。 • DOWN:データリンク層プロトコルのステータスがオフであることを示します。 • DOWN (protocols):インタフェースのデータリンク層がプロトコルモジュールによってシャットダウンされたことを示します。protocols は LAGG などの組み合わせです。 ○ LAGG:集約インタフェースのメンバーポートが選択されていないためにインタフェースがダウンしているデータリンク層を示します
Description	インタフェースの説明
Bandwidth	インタフェースの予想帯域幅

フィールド	説明
Internet protocol processing	インタフェースにIPアドレスが設定されていない場合、インタフェースのネットワークプロトコル設定パラメータ: • Disabled:IP メッセージを処理できません • Enabled:IP メッセージを処理できます。
Internet address:ip-address/mask-length (Type)	インタフェースのIPアドレス。Typeはアドレスの取得方法を示し、値は次のとおりです。 • Primary:手動で構成されたプライマリ・アドレス • Sub:手動で設定されたスレーブアドレス。プライマリ・アドレスが構成されている場合は、プライマリ・アドレスのみが表示されます。この情報は、スレーブアドレスが設定されている場合にのみ表示されます。 • DHCP-allocated:DHCP で取得した IP アドレス。 • BOOTP-allocated:BOOTP で取得した IP アドレス。 • Unnumbered:別のインタフェースの IP アドレスを借用します。 DHCP の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“5 ネットワーク接続”の”DHCP”を参照してください（DHCP 関連は 12 章から 17 章に記載しています）。
IP packet frame type	IPv 4メッセージ送信フレームフォーマット
hardware address	インタフェースのMACアドレス
IPv6 packet frame type	IPv 6メッセージ送信フレームフォーマット
Media type is	インタフェースのメディアタイプ
Port hardware type is	インタフェースのハードウェアタイプ
Port priority	インタフェースプライオリティ
Loopback is set internal	イーサネットインタフェースの内部ループバックテストが実行されています。ユーザの設定に関連する情報が表示されます。
Loopback is set external	イーサネットインタフェースの外部ループバックテストを実行します。このテストは、ユーザの構成に関係します。
Loopback is not set	ループバックテストがインタフェースで設定されていません。ユーザの設定に関連する情報が表示されます。
100 Mbps-speed mode	インタフェース速度は100 Mbpsで、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。
1000 Mbps-speed mode	インタフェース速度は1000 Mbpsで、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。

フィールド	説明
10 Gbps-speed mode	インタフェース速度は10 Gbpsで、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。
Unknown-speed mode	レートネゴシエーションに失敗したか、インタフェースが物理的に接続されていないため、レートは不明です。
half-duplex mode	インタフェースは半二重モードで動作し、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。
full-duplex mode	インタフェースは全二重モードで動作し、ユーザの設定とリンクパラメータのネゴシエーション結果に関する情報が表示されます。
unknown-duplex mode	デュアルモードネゴシエーションが失敗したか、インタフェースが物理的に接続されていないため、不明なデュアルモード
Link speed type is autonegotiation	ユーザがspeed autoを設定した場合に表示されます。
Link speed type is force link	この情報は、ユーザがspeedコマンドを使用して特定のレートを設定した場合に表示されます。たとえば、1000 Mなどです。
link duplex type is autonegotiation	ユーザがduplex autoを設定した場合に表示されます。
link duplex type is force link	この情報は、duplexコマンドを使用してhalfやfullなどの特定のデュプレックスモードが設定されている場合に表示されます。
Maximum frame length	インタフェースが通過できるイーサネットフレームの最大長
Allow jumbo frame to pass	長いフレームの通過を許可
PVID	インタフェースが存在するデフォルトVLAN ID
Port link-type	ユーザの構成に応じて、access、trunk、またはhybridの値を持つリンクタイプ
Tagged VLANs	このインタフェースを介してTagを持つVLAN
UnTagged VLANs	このインタフェースを通過した後にTagを持たないVLAN
VLAN Passing	インタフェースが実際に通過できるVLAN (インタフェースで許可され、作成されたVLAN)
VLAN permitted	インタフェースで許可されているVLANメッセージ
Trunk port encapsulation	Trunkインタフェースのカプセル化形式
Last link flapping	インタフェースの物理状態が最後に変更されてからの経過時間。Neverは、インタフェースがデバイスの起動時からダウンしていることを示します(変わったことはありません)。

フィールド	説明
Last clearing of counters	最後にreset counters interfaceコマンドを使用してインタフェースの統計情報をクリアした時刻(デバイスからの起動時にreset counters interfaceコマンドを実行せずにインタフェースの統計情報をクリアした場合は、Neverと表示されます。)
Current system time	現在のシステム時刻、時刻はYYYY-MM-DD HH:MM:SSの形式で表示されます。 タイムゾーンが構成されている場合は、現在のシステム時刻の後にタイムゾーンを表示する構成がYYYY-MM-DD HH:MM:SS zone-name±HH:MM:SSの形式で追加されます。ここで、zone-nameはローカル・タイムゾーン名です。
Last time when physical state changed to up	最後にインタフェースの物理ステータスがUPになった時刻 タイムゾーンが構成されている場合は、タイムゾーンの構成がYYYY-MM-DD HH:MM:SS zone-name±HH:MM:SSの形式で追加されます。ここで、zone-nameはローカル・タイムゾーン名です。 「-」 は、インタフェースの物理的な状態が変化していないことを示します。
Last time when physical state changed to down	最後にインタフェースの物理状態がDOWNになった時刻 タイムゾーンが構成されている場合は、タイムゾーンの構成がYYYY-MM-DD HH:MM:SS zone-name±HH:MM:SSの形式で追加されます。ここで、zone-nameはローカル・タイムゾーン名です。 「-」 は、インタフェースの物理的な状態が変化していないことを示します。
Last 300 seconds input:0 packets/sec 0 bytes/sec 0% Last 300 seconds output:0 packets/sec 0 bytes/sec 0%	過去300秒間にポートがパケット/秒およびバイト/秒の単位でメッセージを送受信した平均レート、および実際のレートとインタフェース帯域幅の割合 値が 「-」 の場合、統計はサポートされていません
Input (total):0 packets、0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	ポートが受信したメッセージの統計値。通常のメッセージ、例外メッセージ、通常のPAUSEフレームのメッセージ数、バイト数を含む。 ポートが受信するユニキャスト、ブロードキャスト、マルチキャスト、およびPAUSEフレームの数 値が 「-」 の場合、統計はサポートされていません

フィールド	説明
Input (normal):0 packets、0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	ポートが受信した通常のメッセージの統計値。通常のメッセージと通常のPAUSEフレームのメッセージ数、バイト数を含む。 ポートが受信する通常のユニキャスト、ブロードキャスト、マルチキャスト、およびPAUSEフレームの数 値が 「-」 の場合、統計はサポートされていません
input errors	ポートが受信したエラーメッセージの統計値
runts	受信した超小フレームの数 超小フレームとは、64バイト未満で、正しい形式で、有効なCRCフィールドを含むフレームです。
giants	受信したジャンボフレームの数 ジャンボフレームは、ポートが許可する最大メッセージ長よりも長い有効長を持つフレームです。 • 長いフレームが通過できないイーサネットポートの場合、ジャンボフレームとは、有効長が 1518 バイト(なし VLAN Tag)を超えるフレーム、または 1522 バイト(VLAN Tag メッセージ付き)を超えるフレームを指します。 • 長いフレームが通過できるイーサネットポートの場合、ジャンボフレームは指定された最大フレーム長より長い有効長を持つフレームです。
throttles	受信した非整数バイト長のフレームの数
CRC	受信したCRCチェックエラーの正常な長さのフレームの数
frame	受信したCRC検証エラーで、長さが整数バイトではないフレームの数
overruns	ポートの受信レートが受信キューの処理能力を超えると、メッセージがドロップされる

フィールド	説明
aborts	受信した不正メッセージの総数。不正メッセージには次のものが含まれます。 • メッセージフラグメント:長さが 64 バイト未満(長さは整数または整数以外のいずれかです。)で、CRC チェックエラーのあるフレーム • jabber フレーム:有効長がポートが通過できる最大メッセージ長より長く、CRC チェックが正しくないフレーム(長さは、整数バイトまたは非整数バイトのいずれかです。)。長いフレームの通過が禁止されているイーサネットポートの場合、jabber フレームは、1518 (なし VLAN Tag)または 1522 (帯 VLAN Tag)バイトを超える CRC チェックエラーのあるフレームです。長いフレームが通過できるイーサネットポートの場合、jabber フレームは、指定された最大フレーム長よりも長い有効長を持ち、CRC チェックエラーが発生したフレームです。 • シンボルエラーフレーム:メッセージに少なくとも 1 つのエラーが含まれているシンボル • オペコード不明フレーム:メッセージは MAC 制御フレームですが、Pause フレームではありません。 • 長さエラーフレーム:メッセージの長さフィールド 802.3 がメッセージの実際の長さ(46~1500 バイト)と一致しません。
ignored	ポートの受信バッファ不足などによりドロップされたメッセージ数
parity errors	受信したパリティエラーのフレーム数
Output (total):0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	ポートが送信するメッセージの統計値。通常のメッセージ、例外メッセージ、通常のPAUSEフレームのメッセージ数、バイト数を含む。 ポートから送信されるユニキャスト、ブロードキャスト、マルチキャスト、およびPAUSEフレームの数 値が 「-」 の場合、統計はサポートされていません
Output (normal):0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	ポートから送信された通常のメッセージの統計値。通常のメッセージと通常のPAUSEフレームのメッセージ数、バイト数を含む。 ポートから送信される通常のユニキャストメッセージ、ブロードキャストメッセージ、マルチキャストメッセージ、およびPAUSEフレームの数 値が 「-」 の場合、統計はサポートされていません
output errors	各種送信エラーのメッセージ総数

フィールド	説明
underruns	ポートの送信レートが送信キューの処理能力を超え、メッセージがドロップされることは、非常にまれなハードウェア例外です。
buffer failures	ポート送信バッファが不足しているためにドロップされたメッセージの数
aborts	送信に失敗したメッセージの合計数、つまりメッセージの送信が開始されたが、さまざまな理由(例えば)により送信に失敗したメッセージの数
deferred	遅延メッセージの数、遅延メッセージとは送信前に衝突を検出して遅延送信されたメッセージである.
collisions	衝突フレーム数、衝突フレームとは送信中に衝突を検出し、送信を停止したメッセージである.
late collisions	フレームの最初の512 bitsが送信され、衝突が検出されたために送信が遅延された遅延衝突フレームの数
IPv4 traffic statistics	IPv 4メッセージ統計
IPv6 traffic statistics	IPv 6メッセージ統計
Last 300 seconds input rate:0 packets/sec, 0 bytes/sec	過去300秒間にポートが受信したパケット/秒およびバイト/秒の平均レート 値が 「-」 の場合、統計はサポートされていません
Last 300 seconds output rate:0 packets/sec, 0 bytes/sec	過去300秒間にポートが送信したパケット/秒とバイト/秒の平均レート 値が 「-」 の場合、統計はサポートされていません
Input:0 packets, 0 bytes	ポートが受信したメッセージの統計値。メッセージ数、バイト数を含む。 値が 「-」 の場合、統計はサポートされていません
Output:0 packets, 0 bytes	ポートが送信するメッセージの統計値。メッセージ数、バイト数を含む。 値が 「-」 の場合、統計はサポートされていません

#すべてのインタフェースのサマリー情報を表示します。

<AC> display interface brief

Brief information on interfaces in route mode:

Link: ADM - administratively down; Stby - standby

Protocol: (s) – spoofing

Interface	Link	Protocol	Primary IP	Description
GE1/0/1	DOWN	DOWN	--	
Loop0	UP	UP(s)	2.2.2.9	
NULL0	UP	UP(s)	--	
Vlan1	UP	DOWN	--	
Vlan999	UP	UP	192.168.1.42	

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface　　Link Speed　Duplex Type PVID Description
GE1/0/2　　DOWN auto　A　A　1
GE1/0/3　　UP　auto　F(a)　A　1　aaaaaaaaaaaaaaaaaaaaaaaaaa

#ユーザ構成のすべての説明を含む、インタフェース GigabitEthernet1/0/3 のサマリー情報を表示します。

<AC> display interface gigabitethernet 1/0/3 brief description
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface　　Link Speed　Duplex Type PVID Description
GE1/0/3　　UP　auto　F(a)　A　1　aaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

#現在の物理状態が down のインタフェースに関する情報と、down の理由を表示します。

<AC> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface　　Link Cause
GE1/0/1　　DOWN Not connected
Vlan2　　DOWN Not connected

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface　　Link Cause
GE1/0/2　　DOWN Not connected

表 3-2 display interface brief コマンドの表示情報の説明

フィールド	説明
Brief information on interfaces in route mode:	3層モード(route)のインタフェースのサマリー情報、つまり3層インタフェースのサマリー情報

フィールド	説明
リンク:ADM - administratively down;Stby - standby	• インタフェースの Link プロパティの値が「ADM」の場合、そのインタフェースは、shutdown コマンドを使用して管理者によってシャットダウンされました。インタフェース自体の物理状態を復元するには、そのインタフェースで undo shutdown コマンドを実行する必要があります。 • インタフェースの Link プロパティの値が「スティビー」の場合は、そのインタフェースが Standby のバックアップ・インタフェースであることを示します。
Protocol: (s) -spoofing	インタフェースのProtocol属性値に「(s)」が含まれている場合は、そのインタフェースのデータリンク層プロトコルステータスがUPと表示されますが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があります。通常、NULL、LoopBackなどのインタフェースにはこの属性があります。
Interface	インタフェース名の省略名
Link	インタフェースの物理接続ステータス。次の値をとります。 • UP:インタフェースが物理的に接続されていることを示します。 • DOWN:インタフェースが物理的に機能していないことを示します。 • ADM:管理者が shutdown コマンドを使用してインタフェースをシャットダウンしたことを示します。インタフェース自体の物理状態を回復するには、undo shutdown コマンドを実行する必要があります。 • Stby:インタフェースが状態 Standby のバックアップインタフェースであることを示します。

フィールド	説明
Protocol	インタフェースデータリンク層プロトコルの状態。次の値を取ります。 • UP:インタフェースのデータリンク層プロトコルステータスがオンであることを示します。 • DOWN:インタフェースのデータリンク層プロトコルの状態がオフであることを示します • [UP (s)] :インタフェースのデータリンク層プロトコルステータスが [UP] と表示されているが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があります。通常、NULL、LoopBack などのインタフェースはこの値を取ります。
Primary IP	インタフェースのプライマリIPアドレス。値が「--」の場合は、インタフェースにIPアドレスが設定されていません。
Description	インタフェースの説明
Brief information of interfaces in bridge mode:	2層モード(bridge)のインタフェース・サマリー情報、つまり2層インタフェースのサマリー情報
Speed: (a) -auto	インタフェースのSpeedプロパティの値が「(a)」の場合、インタフェースのレートはオートネゴシエーションによって取得されます。 インタフェースのSpeedプロパティの値が「auto」の場合、そのインタフェースのレートは自動ネゴシエーションによって取得されますが、ネゴシエーションはまだ開始されていません。
Duplex: (a) /A - auto;H - half;F - full	インタフェースのDuplex属性の値が「(a)」または 「A」の場合、そのインタフェースのDuplex属性は自動ネゴシエーションによって取得されます。半二重の場合は「H」;「F」 を指定すると全二重になります。 「A」 と表示されている場合は、インタフェースのDuplex属性が自動ネゴシエーションによって取得されたが、ネゴシエーションが開始されていないことを示します。
Type:A - access;T - trunk;H - hybrid	インタフェースのリンクタイプ: • A:Access リンクタイプを示します。 • H:Hybrid リンクタイプを示します。 • T:Trunk リンクタイプを示します。
Speed	インタフェースのビット/秒単位のレート

フィールド	説明
Duplex	インタフェースのデュプレックスモード。値は次のとおりです。 • A:デュプレックスモードがオートネゴシエーションの結果によって決定されることを示します。 • F:全二重を表します。 • F (a) :自由ネゴシエーションの結果が全二重であることを示す. • H:半二重 • H (a) :自由ネゴシエーションの結果が半二重であることを示す.
Type	インタフェースのリンクタイプ: • A:Access リンクタイプを示します。 • H:Hybrid リンクタイプを示します。 • T:Trunk リンクタイプを示します。
PVID	インタフェースが存在するデフォルトVLAN ID
Cause	インタフェースの物理接続ステータスがdownである理由は、次のとおりです。 • Administratively:このリンクが手動でダウンしたことを示します(shutdown コマンドが設定されました)。実際の物理状態に戻すには、undo shutdown コマンドを実行する必要があります。 • DOWN (Link-Aggregation interface down):集約インタフェースがダウンすると、その集約インタフェースのすべてのメンバーポートのステータスが DOWN と表示され、ダウンの理由が DOWN (Link-Aggregation interface down)と表示されます。 • DOWN (Loopback detection down):ループ検出モジュールがループを検出したため、インタフェースが自動的にシャットダウンされました • Not connected:物理的な接続がないことを示します(ネットワークケーブルが接続されていないか、ネットワークケーブルに問題がある可能性があります。)。 • STP DOWN:STP BPDU 保護がトリガーされたためにインタフェースが自動的にシャットダウンされました • Standby:インタフェースがバックアップ状態であることを示します。

関連コマンド

- **reset counters interface**

3.1.3 duplex

Syntax

duplex { **auto** | **full** | **half** }

undo duplex

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auto:インタフェースは、デュプレックス状態をピアインタフェースと自動的にネゴシエートします。

full:パケットを送信している間にインタフェースがパケットを受信できる全二重状態。

half:半二重状態で、インタフェースは同時刻にのみパケットを送信または受信できる。

説明

duplex コマンドを使用して、イーサネットインタフェースのデュプレックスモードを設定します。

undo duplex コマンドを使用して、デフォルトの状態を復元します。

例

#ギガビットイーサネット 1/0/1 をデュプレックスモードで動作するように設定します。
<AC> system-view

[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] duplex full

3.1.4 flow-interval

Syntax

flow-interval *interval*

undo flow-interval

デフォルト

インタフェース統計メッセージの間隔は 300 秒です。

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval:インタフェース統計のインターバル値。5~300 の範囲の値で、単位は秒、ステップサイズは 5 (つまり、値は 5 の整数倍でなければなりません)です。

説明

flow-interval コマンドを使用して、インタフェース統計情報の間隔を設定します。

undo flow-interval コマンドを使用して、デフォルトの状態を復元します。

例

#イーサネットインタフェース GigabitEthernet1/0/1 の統計情報間隔を 100 秒に設定します。

<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] flow-interval 100

3.1.5 interface

Syntax

interface *interface-type* { *interface-number* | *interface-number.subnumber* }

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type:インタフェースのタイプを指定します。

interface-number:インタフェース番号を指定します。

interface-number.subnumber:サブインタフェース番号を指定します。ここで、interface-number はプライマリインタフェース番号です。subnumber はサブインタフェース番号で、値の範囲は 1~4094 です。

説明

interface コマンドを使用して、インタフェースビューにアクセスするか、サブインタフェースを作成してサブインタフェースビューにアクセスします。指定したサブインタフェースがすでに存在する場合は、サブインタフェースビューに直接進みます。

例

#イーサネットインタフェース GigabitEthernet1/0/1 ビューに入ります。

<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1]

#イーサネットサブインタフェース GigabitEthernet1/0/1.1 を作成し、サブインタフェースのビューに入ります。

<AC> system-view
[AC] interface gigabitethernet 1/0/1.1
[AC-GigabitEthernet1/0/1.1]

3.1.6 jumboframe enable

Syntax

jumboframe enable [*size*]

undo jumboframe enable [*size*]

デフォルト

デバイスでは、最大長が 4000 バイトの非常に長いフレームを通過させることができます。

View

Layer 2 Ethernet interface view

Layer 3 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

size:イーサネットインタフェースで通過できるジャンボフレームの最大長（バイト単位）を設定します。このパラメータの範囲は 1700~4000 です。偶数のみ指定が可能です。

説明

jumboframe enable コマンドを使用すると、非常に長いフレームを通過させることができます。

undo jumboframe enable *size* コマンドを使用して、デフォルトの状態を復元します。**undo jumboframe enable** コマンドは、長いフレームの通過を禁止するために使用します。**undo** コマンドで *size* を指定しない場合は 1700 バイトに設定します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

🕮 **メモ** :

size で指定する値は VLAN タグを含みます。

例

#イーサネットインタフェース GigabitEthernet1/0/1 を介してジャンボフレームを許可します。

<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] jumboframe enable

3.1.7 loopback

Syntax

loopback { **external** | **internal** }

デフォルト

イーサネットインタフェースのループバック機能がオフになっています。

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

external:イーサネットインタフェースの外部ループバック機能をオンにします。

internal:イーサネットインタフェースの内部ループバック機能をオンにします。

説明

🕮 **メモ** :

ループバック機能をオンにすると、インタフェースはパケットを正常に転送できなくなります。必要に応じて設定してください。

loopback コマンドを使用して、イーサネットインタフェースのループバック機能をオンにします。

ループバック機能をオンにすると、インタフェースは自動的に全二重モードに切り替わり、ループバック機能をオフにすると、自動的に元の二重モードに戻ります。

shutdown および **loopback** コマンドは相互に排他的であり、設定に失敗します。

例

#イーサネットインタフェース GigabitEthernet1/0/1 の内部ループバック機能をオンにします。

<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] loopback internal

3.1.8 multicast-suppression

🕮 **メモ**:

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

multicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo multicast-suppression

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio: マルチキャスト抑制しきい値をインタフェース帯域幅のパーセンテージで設定します。この引数の値の範囲は 0 から 100 です。値が小さいほど、通過できるマルチキャストトラフィックは少なくなります。

pps *max-pps*: インタフェースが毎秒転送できるマルチキャストパケットの最大数を指定します。max-pps 引数の値の範囲 (pps 単位) は、0 から 1.4881×インタフェース帯域幅です。

kbps *max-kbps*: Ethernet インタフェースが 1 秒あたりに転送できるマルチキャストトラフィックの最大キロビット数を指定します。この引数の値の範囲 (kbps) は、0～インタフェース帯域幅です。

説明

multicast-suppression コマンドを使用して、マルチキャストストーム抑制を有効にし、マルチキャスト抑制しきい値を設定します。

undo multicast-suppression コマンドを使用して、マルチキャストストーム抑制を無効にします。

マルチキャストストーム抑制機能は、マルチキャストトラフィックのサイズをインタフェース上のしきい値に制限します。インタフェース上のブロードキャストトラフィックがこのしきい値を超えると、トラフィックがこのしきい値を下回るまでシステムはパケットを破棄します。

multicast-suppression コマンドはマルチキャストトラフィックを物理的に抑制するためにチップを使用します。

pps または **kbps** で設定された抑制しきい値は、チップでサポートされているステップの倍数に変換される場合があります。その結果、有効な抑制しきい値が設定されたものと異なる場合があります。有効な抑制しきい値を確認するには、装置のプロンプトを参照してください。

例

#ギガビットイーサネット 1/0/1 でマルチキャストストーム抑制閾値を 10000kbps に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] multicast-suppression kbps 10000

3.1.9 port link-mode

Syntax

port link-mode bridge

undo port link-mode

デフォルト

bridge

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

bridge:レイヤ 2 モードで動作します。

説明

port link-mode コマンドを使用して、イーサネットインタフェースの動作モードを切り替えます。

undo port link-mode コマンドを使用して、デフォルトの状態を復元します。

注意

QX-W2300AC シリーズは bridge モードのみサポートしています。

例

#インタフェース GigabitEthernet1/0/1 をレイヤ 2 モードで動作させます。

```
<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] port link-mode bridge
```

3.1.10 speed

Syntax

speed { **100** | **1000** | **10000** | **auto** }

undo speed

デフォルト

イーサネットインタフェースの速度は auto 状態です。

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

100:インタフェースレートが 100 Mbps に設定します。

1000:インタフェースレートが 1000 Mbps に設定します。

10000:インタフェースレートが 10000 Mbps に設定します。

auto: インタフェースがピアと速度をネゴシエートできるようにします。

説明

speed コマンドを使用して、イーサネットインタフェースの速度を設定します。

undo speed コマンドを使用して、デフォルトの状態を復元します。

イーサネット銅線ポートの場合、**speed** コマンドを使用して、ピアインタフェースの速度に一致する速度を設定します。このコマンドのキーワードに対する銅線ポートのサポートは、銅線ポートタイプによって異なります。詳細については、**speed ?**コマンドをインタフェースビューで実行します。銅線ポートの速度を設定したときに、操作が失敗したことを示すメッセージが表示されない場合、銅線ポートはこの速度をサポートします。それ以外の場合、銅線ポートはこの速度をサポートしません。

ファイバポートの場合、**speed** コマンドを使用して、トランシーバモジュールのレートに一致する速度を設定します。このコマンドのキーワードに対するファイバポートのサポートは、ファイバポートのタイプによって異なります。詳細については、**speed ?**コマンドをインタフェースビューで実行します。ファイバポートの速度を設定するときに、操作が失敗したことを示すメッセージが表示されない場合、ファイバポートはこの速度をサポートします。それ以外の場合、ファイバポートはこの速度をサポートしません。

また、トランシーバモジュールが正しく使用できるように、取り付けられているトランシーバモジュールに応じてファイバポートの速度を選択する必要があります。ファイバポートに取り付けられているトランシーバモジュールがファイバポートの速度をサポートしていない場合、トランシーバモジュールは使用できません。たとえば、次の条件が存在する場合、トランシーバモジュールは使用できません。

- SFP+ファイバポートに取り付けられているトランシーバモジュールは SFP GE トランシーバモジュールであり、ファイバポートで **speed 10000** コマンドが実行されます。
- SFP+ファイバポートに取り付けられているトランシーバモジュールは SFP 10-GE トランシーバモジュールであり、**speed 1000** コマンドはファイバポートで実行されます。

speed 10000 コマンドは、EWPXM3XG03 Ethernet インタフェース拡張モジュールが実装されている場合にのみデバイスでサポートされます。

例

#イーサネットインタフェース GigabitEthernet1/0/1 のレートをオートネゴシエーションに設定します。

<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] speed auto

3.1.11 unicast-suppression

🕮 **メモ**：

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

unicast-suppression { *ratio* | **pps** *max-pps* | **kbps** *max-kbps* }

undo unicast-suppression

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio: 未知のユニキャスト抑制しきい値をインタフェース帯域幅のパーセンテージで設定します。この引数の値の範囲は 0 から 100 です。値が小さいほど、通過できる未知のユニキャストトラフィックは少なくなります。

pps *max-pps*: インタフェースが毎秒転送できる未知のユニキャストパケットの最大数を指定します。max-pps 引数の値の範囲 (pps 単位) は、0 から 1.4881×インタフェース帯域幅です。

kbps *max-kbps*: Ethernet インタフェースが 1 秒あたりに転送できる未知のユニキャストトラフィックの最大キロビット数を指定します。この引数の値の範囲 (kbps) は、0～インタフェース帯域幅です。

説明

unicast-suppression コマンドを使用して、未知のユニキャストストーム抑制を有効にし、未知のユニキャスト抑制しきい値を設定します。

undo unicast-suppression コマンドを使用して、未知のユニキャストストーム抑制を無効にします。

未知のユニキャストストーム抑制機能は、未知のユニキャストトラフィックのサイズをインタフェース上のしきい値に制限します。インタフェース上の未知のユニキャストトラフィックがこのしきい値を超えると、トラフィックがこのしきい値を下回るまでシステムはパケットを破棄します。

unicast-suppression コマンドは未知のユニキャストトラフィックを物理的に抑制するためにチップを使用します。

pps または **kbps** で設定された抑制しきい値は、チップでサポートされているステップの倍数に変換される場合があります。その結果、有効な抑制しきい値が設定されたものと異なる場合があります。有効な抑制しきい値を確認するには、装置のプロンプトを参照してください。

例

#ギガビットイーサネット 1/0/1 で未知のユニキャストストーム抑制閾値を 10000kbps に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] unicast-suppression kbps 10000

目次

このセクションのページは **4-x-x** です。

4 章 Interface range 4-1
4.1 Interface range コマンド 4-1
4.1.1 display interface range 4-1
4.1.2 interface range 4-2
4.1.3 interface range name 4-3

4章 Interface range

4.1 Interface rangeコマンド

4.1.1 display interface range

Syntax

display interface range [**name** *name*]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

name *name*:デバイス上に作成されたバルクインタフェースの別名。1~32 文字の文字列で、大文字と小文字が区別されます。このパラメータを指定しない場合は、**interface range name** コマンドで作成された、現在のデバイスのすべてのバルクインタフェースの情報が表示されます。

説明

display interface range コマンドは、**interface range name** コマンドで作成されたバルクインタフェースの情報を表示するために使用されます。

例

#interface range name コマンドで作成された、現在のデバイスのすべてのバルクインタフェースに関する情報を表示します。

<Sysname> display interface range

Interface range name t2 GigabitEthernet1/0/1 to GigabitEthernet1/0/2

Interface range name test GigabitEthernet1/0/3 to GigabitEthernet1/0/4

上記の情報は、インタフェース GigabitEthernet1/0/1 と GigabitEthernet1/0/2 がバルクインタフェース t2 にバインドされ、インタフェース GigabitEthernet1/0/3 と GigabitEthernet1/0/4 がバルクインタフェース test にバインドされていることを示しています。

関連コマンド

- **interface range name**

4.1.2 interface range

Syntax

interface range *interface-list*

View

System view

定義済みユーザーロール

network-admin

パラメータ

interface-list:interface-list ={interface-type interface-number1 [to interface-type interface-number2]}&<1-24>で表されるインタフェースのリスト。ここで、interface-type interface-number はインターフェイスタイプとインタフェース番号を表します。&<1-24>は、前のパラメータが最大 24 回入力できることを示します。interface-type interface-number2 の値は interface-type interface-number1 の値以上です。選択したインタフェースは、同じインタフェースカード上にある必要があります。

説明

interface range コマンドを使用してインタフェースのグループをバインドし、インタフェースのバルク設定ビューに移動します。

複数のインタフェースで特定の機能(例えば shutdown)を設定する必要がある場合は、インタフェースビューに 1 つずつアクセスし、各インタフェースでコマンドを実行する必要があります。**interface rang**e コマンドは、一括設定を提供します。このコマンドを使用して、さまざまなタイプのインタフェースをバインドし、インタフェースのバルク構成ビューに移動します。

インタフェースのバルク構成ビューでは、インタフェースリストの最初のインタフェースでサポートされているコマンドのみを実行できます。最初のインタフェースではサポートされていないが、他のメンバーインタフェースではサポートされているコマンドは実行できません。(インタフェースリストの最初のインタフェースとは、**interface range** コマンドの実行時に指定されたインタフェースをアルファベット順に小さい順に並べたものです。)。[Interface Bulk Configuration] ビューで、疑問符を入力して [Enter] を押すと、そのビューでサポートされているすべてのコマンドが表示されます。

インタフェースのバルク構成ビューでコマンドを実行すると、バインドされたすべてのインタフェースでコマンドが実行されます。

- コマンドの実行が完了すると、設定は失敗し、インタフェースバルク設定ビューにとどまります。
  - 設定に失敗したインタフェースがインタフェースリストの最初のインタフェースである場合は、リスト内のすべてのインタフェースでコマンドが設定されていません。

- ○ 設定に失敗したインタフェースが別のインタフェースである場合は、失敗したインタフェース以外のインタフェースは設定に成功しています。
- コマンドの実行が完了してシステムビューに戻ると、次のように表示されます。
- ○ このコマンドは、インタフェースビューとシステムビューの両方でサポートされています。
- ○ リスト内のインタフェースの 1 つで構成に失敗し、システムビューで構成に成功しました。
- ○ リスト内でこのインタフェースの背後にあるインタフェースは、コマンドを実行しなくなりました。

この時点で、リスト内の各インタフェースのビューで display this コマンドを使用して構成を確認し、システムビューで構成する必要がない場合は、適切な undo コマンドを使用して構成をキャンセルします。

[Interface Bulk Configuration] ビューで、**display this** コマンドを実行すると、インタフェースリストの最初のインタフェースで現在有効な設定が表示されます。

インタフェースのバルク構成には、次の制限があります。

- インタフェースリストの最初のインタフェースに設定する前に、**interface interface-type interface-number** コマンドでインタフェースビューにアクセスできることを確認する必要があります。
- 集約ポートがバルクインタフェースに結合されている場合は、その集約ポートのメンバーインタフェースを結合しないことをお勧めします。結合されていないと、バルクインタフェース設定ビューで特定の設定コマンドを実行したときに、集約が分割される可能性があります。
- バルクインタフェースに含まれるインタフェースの数に上限はなく、システムリソースによってのみ制限されます。インタフェースの数が多い場合、バルクインタフェース設定ビューでコマンドを実行すると待機時間が長くなります。

例

#インタフェース GigabitEthernet1/0/1 から GigabitEthernet1/0/5 をシャットダウンします。

```
<Sysname> system-view
[Sysname] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[Sysname-if-range] shutdown
```

4.1.3 interface range name

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

View

System view

定義済みユーザーロール

network-admin

パラメータ

name:バルクインタフェースの別名。1~32 文字の文字列で、大文字と小文字が区別されます。

*interface-lis*t:interface-list ={interface-type interface-number [to interface-type interface-number]}&<1-24>で表されるインタフェースのリスト。ここで、interface-type interface-number はインターフェイスタイプとインタフェース番号を表します。&<1-24>は、前のパラメータが最大 24 回入力できることを示します。interface-type interface-number2 の値は interface-type interface-number1 の値以上です。選択したインタフェースは、同じインタフェースカード上にある必要があります。

説明

interface range name name interface interface-list コマンドを使用してインタフェースのグループをバインドし、そのグループにエイリアスを割り当て、そのエイリアスを使用してインタフェースのバルク構成ビューにアクセスします。

interface range name name (interface パラメータを指定しない場合)コマンドは、エイリアスを使用してインタフェースバルク設定ビューにアクセスするために使用されます。

undo interface range name コマンドを使用すると、インタフェースのバインドが解除され、インタフェースのエイリアスが削除されます。

interface range name コマンドと **interface range** コマンドはともにインタフェースの一括設定機能を提供し、それらの違いは以下のとおりである:**interface range name** コマンドはインタフェースをバインドする時に 1 つの別名を定義することができ、複数回のバインドを行うことができ、異なるバインドに異なる別名を定義し、区別を示し、記憶しやすい。また、エイリアスを使用してインタフェースのバルク構成ビューに直接入力できるため、インタフェースの長いリストを出力する必要がなくなり、構成が簡単になります。**display interface range** コマンドを使用すると、どのインタフェースがバインドされているかを確認できます。

インタフェースのバルク構成ビューでは、インタフェースリストの最初のインタフェースでサポートされているコマンドのみを実行できます。最初のインタフェースではサポートされていないが、他のメンバーインタフェースではサポートされているコマンドは実行できません。(インタフェースリストの最初のインタフェースとは、**interface range** コマンドの実行時に指定されたインタフェースをアルファベット順に小さい順に並べたものです。)。[Interface Bulk Configuration] ビューで、疑問符を入力して [Enter] を押すと、そのビューでサポートされているすべてのコマンドが表示されます。

インタフェースのバルク構成ビューでコマンドを実行すると、バインドされたすべてのインタフェースでコマンドが実行されます。

- コマンドの実行が完了すると、設定は失敗し、インタフェースバルク設定ビューにとどまります。

- 設定に失敗したインタフェースがインタフェースリストの最初のインタフェースである場合は、リスト内のすべてのインタフェースでコマンドが設定されていません。
- 設定に失敗したインタフェースが別のインタフェースである場合は、失敗したインタフェース以外のインタフェースは設定に成功しています。

- コマンドの実行が完了してシステムビューに戻ると、次のように表示されます。

- このコマンドは、インタフェースビューとシステムビューの両方でサポートされています。
- リスト内のインタフェースの 1 つで構成に失敗し、システムビューで構成に成功しました。
- リスト内でこのインタフェースの背後にあるインタフェースは、コマンドを実行しなくなりました。

この時点で、リスト内の各インタフェースのビューで display this コマンドを使用して構成を確認し、システムビューで構成する必要がない場合は、適切な undo コマンドを使用して構成をキャンセルします。

[Interface Bulk Configuration] ビューで、**display this** コマンドを実行すると、インタフェースリストの最初のインタフェースで現在有効な設定が表示されます。

インタフェースのバルク構成には、次の制限があります。

- インタフェースリストの最初のインタフェースに設定する前に、**interface interface-type interface-number** コマンドでインタフェースビューにアクセスできることを確認する必要があります。
- 集約ポートがバルクインタフェースに結合されている場合は、その集約ポートのメンバーインタフェースを結合しないことをお勧めします。結合されていないと、バルクインタフェース設定ビューで特定の設定コマンドを実行したときに、集約が分割される可能性があります。
- バルクインタフェースに含まれるインタフェースの数に上限はなく、システムリソースによってのみ制限されます。インタフェースの数が多い場合、バルクインタフェース設定ビューでコマンドを実行すると待機時間が長くなります。
- システムでサポートされるバルクインタフェースエイリアスの数に上限はなく、システムリソースによってのみ制限されます。推奨ユーザ数は 1000 以下で、構成数が多すぎると、この機能の実行効率が低下する可能性があります。

例

#5 つの Ethernet インタフェース GigabitEthernet1/0/1~GigabitEthernet1/0/5 を myEthPort として定義し、 [Bulk Interface] ビューに移動します。

```
<Sysname> system-view
[Sysname] interface range name myEthPort interface gigabitethernet 1/0/1 to gigabitethernet 1/0/5
[Sysname-if-range-myEthPort]
```

#myEthPort エイリアスに対応するバルクインタフェース設定ビューを入力します。

```
<Sysname> system-view
```

[Sysname] interface range name myEthPort
[Sysname-if-range-myEthPort]

関連コマンド

- **display interface range**

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

5. ネットワーク接続

本マニュアルは以下に示す章で構成されています。

01-MAC アドレステーブル

02-リンクアグリゲーション

03-VLAN

04-ループ検出

05-STP

06-LLDP

07-レイヤ 2 フォワーディング

08-ARP

09-Gratuitous ARP

10-Proxy ARP

11-IP アドレス

12-DHCP 共通

13-DHCP サーバ

14-DHCP リレー

15-DHCP クライアント

16-BOOTP クライアント

17-DHCP スヌーピング

18-DNS

19-HTTP

20-IP パフォーマンスの最適化

21-NAT

22-IP ルーティングの基本

23-スタティックルーティング

24-IGMP スヌーピング

目次

このセクションのページは **5-x-x** です。

1 章 MAC アドレステーブル 1-1
1.1 MAC アドレステーブルコマンド 1-1
1.1.1 display mac-address 1-1
1.1.2 display mac-address aging-time 1-3
1.1.3 display mac-address mac-learning 1-4
1.1.4 display mac-address mac-move 1-5
1.1.5 mac-address (interface view) 1-6
1.1.6 mac-address (system view) 1-7
1.1.7 mac-address mac-learning enable 1-9
1.1.8 mac-address max-mac-count 1-11
1.1.9 mac-address max-mac-count enable-forwarding 1-12
1.1.10 mac-address notification mac-move 1-13
1.1.11 mac-address notification mac-move suppression (interface view) 1-14
1.1.12 mac-address notification mac-move suppression (system view) 1-15
1.1.13 mac-address timer 1-16
1.1.14 snmp-agent trap enable mac-address 1-17

1章 MAC アドレステーブル

🕮 メモ ：

このセクションでは、ユニキャストのスタティック MAC アドレステーブルエントリ、ダイナミック MAC アドレステーブルエントリ、およびブラックホール MAC アドレステーブルエントリの設定についてのみ説明します。

1.1 MACアドレステーブルコマンド

1.1.1 display mac-address

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address:指定された MAC アドレスの MAC アドレステーブルエントリを表示します。mac-address は H-H-H の形式です。設定時に、ユーザは、MAC アドレスの各セグメントの先頭の 「0」 を省略することができ、例えば、入力された MAC アドレスが「000f-00e2-0001」であることを示す「f-e2-1」を入力する。

vlan vlan-id:指定した VLAN の MAC アドレステーブルエントリを表示します。vlan-id の値の範囲は 1~4094 です。

dynamic:ダイナミック MAC アドレステーブルエントリを表示します。

static:スタティック MAC アドレステーブルエントリを表示します。

interface *interface-type interface-number*:指定したインタフェースの MAC アドレステーブルエントリを表示します。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。

blackhole:ブラックホール MAC アドレステーブルエントリを表示します。

count:MAC アドレステーブルエントリの数を表示します。このパラメータを設定すると、条件を満たす(count の前のパラメータによって決定されます。) MAC アドレステーブル

エントリの数のみが表示され、MAC アドレステーブルエントリの内容は表示されません。このパラメータを指定しない場合は、該当する MAC アドレステーブルの内容が表示されます。

説明

display mac-address コマンドは、MAC アドレステーブル情報を表示します。このコマンドを使用して、MAC アドレス、VLAN ID、インタフェースなどの情報を含む静的、動的、ブラックホール MAC アドレステーブルエントリを表示します。

パラメータを指定しない場合は、すべての MAC アドレステーブルエントリ情報が表示されます。

集約インタフェースの場合、MAC アドレステーブルエントリに集約インタフェースのダイナミック MAC アドレスを表示するには、ポートを選択する必要があります。

例

#VLAN 100 の MAC アドレステーブルエントリの情報を表示します。

<Sysname> display mac-address vlan 100

```
MAC Address     VLAN ID    State          Port/Nickname          Aging
                                       GE1/0/2
0033-0033-0033   100       Blackhole       N/A                   N
0000-0000-0002   100       Static          GE1/0/3               N
00e0-fc00-5829   100       Learned         GE1/0/4               Y
```

#MAC アドレステーブルエントリの数を表示します。

<Sysname> display mac-address count

```
1 mac address (es) found.
```

表1-1 display mac-address コマンドの表示情報の説明

フィールド	説明
MAC Address	MACアドレス
VLAN ID	MACアドレス対応インタフェースが属するVLAN
State	次のようなMACアドレステーブルエントリのステータス。 ● Static:テーブルエントリがスタティックMACアドレステーブルエントリであることを示します。 ● Learned:ダイナミックMACアドレステーブルエントリ。手動で設定することも、デバイスから学習することもできます。 ● Blackhole:エントリがブラックホールMACアドレステーブルエントリであることを示します。 ● Security:ポートセキュリティ機能で設定または学習されたMACアドレステーブルエントリであることを示します。

フィールド	説明
Port/Nickname	MACアドレスに対応するインタフェース名このMACアドレス宛てのメッセージがこのインタフェースから送信されることを示します(ブラックホールMACアドレステーブルエントリここではN/Aと表示されています)。
Aging	エージング時間。このテーブルエントリには2つの値があります。 • Y:テーブルエントリがエージングされることを示します。 • N:テーブル・エントリがエージングされないことを示します。
n mac address (es) found	合計n個のMACアドレステーブルエントリ

関連コマンド

- mac-address
- mac-address timer

1.1.2 display mac-address aging-time

Syntax

display mac-address aging-time

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mac-address aging-time コマンドは、MAC アドレステーブルの動的テーブルエントリの経過時間を表示します。

例

#MAC アドレステーブルの動的テーブルエントリのエージングタイムを表示します。

<Sysname> display mac-address aging-time

```
MAC address aging time:300 s.
```

関連コマンド

- mac-address timer

1.1.3 display mac-address mac-learning

Syntax

display mac-address mac-learning [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースの MAC アドレス学習ステータスを表示します。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。このパラメータを指定しない場合、グローバルおよびすべてのインタフェースの MAC アドレス学習ステータスが表示されます。

説明

display mac-address mac-learning コマンドは、MAC アドレス学習機能のオン状態を表示します。

例

#グローバルおよびすべてのインタフェースの MAC アドレス学習ステータスを表示します。

<Sysname> display mac-address mac-learning

```
Global MAC address learning status: Enabled.

Port                    Learning Status
GE1/0/1                  Enabled
GE1/0/2                  Enabled
```

表1-2 display mac-address mac-learning コマンドの表示情報の説明

フィールド	説明
Global MAC address learning status	グローバルMACアドレス学習ステータス:Enabledはオン、Disabledはオフ
Port	インタフェース名
Learning Status	インタフェースのMACアドレス学習ステータス:Enabledはオン、Disabledはオフ

関連コマンド

- mac-address mac-learning enable

1.1.4 display mac-address mac-move

Syntax

display mac-address mac-move

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mac-address mac-move は MAC アドレス移動レコードを表示します。

MAC アドレスが 2 つのインタフェース間を頻繁に移動すると、ネットワークでレイヤ 2 ループが発生することがあります。ループを検出して見つけるには、MAC アドレス移動レコードを表示します。

MAC アドレス移動レコードでは、同じ MAC アドレス、VLAN、送信元ポート、および現在のポートを持つレコードは 1 つのレコードと見なされます。

デバイスは、最大 200 個の MAC アドレス移動レコードを保存できます。

例

MAC アドレス移動レコードを表示します。

<Sysname> display mac-address mac-move

```
MAC address    VLAN Current port  Source port   Last time          Times
0000-0001-002c 1    GE1/0/1       GE1/0/2       2013-05-20 13:40:52 20
0000-0001-002c 1    GE1/0/2       GE1/0/1       2013-05-20 13:41:32 20
0000-0094-0001 1    GE1/0/3       GE1/0/4       2013-05-20 13:42:22 13
0000-0094-0001 1    GE1/0/4       GE1/0/3       2013-05-20 13:42:21 12
---  4 MAC address moving records found  ---
```

表1-3 display mac-address mac-move コマンドの表示情報の説明

フィールド	説明
VLAN	MACアドレスエントリの送信インタフェースが属するVLAN
Current port	MACアドレスの移動先のインタフェース

フィールド	説明
Source port	MACアドレスの移動元のインタフェース
Last time	MACアドレスが最後に移動された時刻
Times	デバイスの起動後にMACアドレスが移動した回数。 MACアドレスレコードの場合、新しいMACアドレスの移動にMACアドレスレコードと同じMACアドレス、VLAN、Current Port、およびSource Portの各フィールドが含まれていると、MACアドレスの移動回数が1増加します。

関連コマンド

- mac-address notification mac-move

1.1.5 mac-address (interface view)

Syntax

mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

デフォルト

インタフェースで MAC アドレステーブルエントリが設定されていません。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

dynamic:ダイナミック MAC アドレステーブルエントリ。

static:スタティック MAC アドレステーブルエントリ。

mac-address:H-H-H 形式の MAC アドレス。マルチキャスト MAC アドレス、すべて 0 の MAC アドレス、およびすべて F の MAC アドレスはサポートされません。設定時に、ユーザは、MAC アドレスの各セグメントの先頭の 「0」 を省略することができ、例えば、入力された MAC アドレスが「000 f-00e2-0001」であることを示す「f-e2-1」を入力する。

vlan *vlan-id*:現在のインタフェースが属する VLAN。vlan-id は指定された VLAN の番号で、範囲は 1~4094 です。VLAN はすでに作成されている必要があります。

説明

mac-address コマンドは、インタフェースで MAC アドレステーブルエントリを追加または変更するために使用します。

undo mac-address コマンドを使用して、インタフェースの MAC アドレステーブルエントリを削除します。

通常、デバイスは、送信元 MAC アドレス学習プロセスによって MAC アドレステーブルを自動的に作成します。インタフェースのセキュリティを強化するために、ネットワーク管理者は、MAC アドレステーブルに特定の MAC アドレステーブルエントリを手動で追加し、ユーザデバイスをインタフェースにバインドして、不正なユーザによるデータの不正取得を防ぐことができます。手動で設定されたスタティック MAC アドレステーブルエントリは、自動生成されたテーブルエントリよりも優先されます。

構成を保存しないと、デバイスの再起動後にすべてのテーブルエントリが失われます。設定を保存すると、スタティック MAC アドレステーブルエントリは失われず、ダイナミック MAC アドレステーブルエントリは失われます。

例

#VLAN 2 に属するポート GigabitEthernet1/0/1 の下で静的 MAC アドレステーブルエントリ 000 f-e201-0101 を追加して下さい。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2

#VLAN 1 に属するインタフェース Bridge-Aggregation1 の下で静的 MAC アドレステーブルエントリ 000 f-e201-0102 を追加して下さい。

<Sysname> system-view

[Sysname] interface bridge-aggregation 1

[Sysname-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1

関連コマンド

- display mac-address
- mac-address (system view)

1.1.6 mac-address (system view)

Syntax

mac-address { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

mac-address blackhole *mac-address* **vlan** *vlan-id*

undo mac-address [[**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

デフォルト

MAC アドレステーブルエントリが設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

dynamic:ダイナミック MAC アドレステーブルエントリ。

static:スタティック MAC アドレステーブルエントリ。

blackhole:ブラックホール MAC アドレステーブルエントリ。メッセージの送信元または宛先 MAC アドレスがブラックホール MAC アドレステーブルエントリと一致すると、そのメッセージはドロップされます。

mac-address:H-H-H 形式の MAC アドレス。マルチキャスト MAC アドレス、すべて 0 の MAC アドレス、およびすべて F の MAC アドレスはサポートされません。設定時に、ユーザは、MAC アドレスの各セグメントの先頭の 「0」 を省略することができ、例えば、入力された MAC アドレスが「000 f-00e2-0001」であることを示す「f-e2-1」を入力する。

vlan *vlan-id*:インタフェースが属する VLAN を指定します。vlan-id は指定された VLAN の番号で、範囲は 1~4094 です。VLAN はすでに作成されている必要があります。

interface *interface-type interface-number*:出力インタフェース。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。

説明

mac-address コマンドを使用して、MAC アドレステーブルエントリを追加または変更します。

undo mac-address コマンドを使用して、MAC アドレステーブルエントリを削除します。

このコマンドでは、次のタイプの MAC アドレステーブルエントリを追加または変更できます。

ダイナミック MAC アドレス:デバイスは、送信元 MAC アドレス学習プロセスによって MAC アドレステーブルを自動的に作成するか、ユーザが手動で設定します。

静的 MAC アドレス:ネットワーク管理者は、インタフェースのセキュリティを強化するために、MAC アドレステーブルに特定の MAC アドレステーブルエントリを手動で追加し、ユーザデバイスをインタフェースにバインドして、不正なユーザによるデータの不正取得を防止できます。手動で設定されたスタティック MAC アドレステーブルエントリは、自動生成されたテーブルエントリよりも優先されます。

ブラックホール MAC アドレス:送信元または宛先 MAC アドレスを指定するメッセージをドロップします。

ユーザが手動で設定したスタティック MAC アドレステーブルエントリまたはブラックホール MAC アドレステーブルエントリは、ダイナミック MAC アドレステーブルエントリによって上書きされません。ダイナミック MAC アドレステーブルエントリは、スタティック MAC アドレステーブルエントリおよびブラックホール MAC アドレステーブルエントリによって上書きできます。

MAC アドレステーブルエントリを削除する場合は、次の点に注意してください。

- パラメータを指定せずに undo mac-address コマンドを実行すると、すべてのユニキャスト MAC アドレステーブルエントリとスタティックマルチキャスト MAC アドレステーブルエントリが削除されます。
- 指定した VLAN のすべての MAC アドレステーブルエントリを削除できます(ユニキャスト MAC アドレステーブルエントリとスタティックマルチキャスト MAC アドレステーブルエントリを含む)。オプションで、ダイナミック MAC アドレステーブルエントリ、スタティック MAC アドレステーブルエントリ、ブラックホール MAC アドレステーブルエントリを削除できます。ユニキャスト MAC アドレステーブルエントリはインタフェースごとに削除できますが、マルチキャスト MAC アドレステーブルエントリはインタフェースごとに削除できません。

構成を保存しないと、デバイスの再起動後にすべてのテーブルエントリが失われます。設定を保存すると、静的 MAC アドレステーブルエントリ、ブラックホール MAC アドレステーブルエントリ、動的テーブルエントリは失われません。

例

#宛先 MAC アドレスが 000 f-e201-0101、送信インタフェースが GigabitEthernet1/0/1 で、VLAN 2 に属する静的アドレステーブルエントリを追加します。

<Sysname> system-view

[Sysname] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2

関連コマンド

- display mac-address
- mac-address (interface view)

1.1.7 mac-address mac-learning enable

Syntax

mac-address mac-learning enable

undo mac-address mac-learning enable

デフォルト

MAC アドレス学習機能がオンになっています。

View

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-address mac-learning enable コマンドを使用して、デバイスのグローバル、インタフェース、または VLAN の MAC アドレス学習機能を有効にします。

undo mac-address mac-learning enable コマンドを使用して、デバイスのグローバル、インタフェース、または VLAN の MAC アドレス学習機能をオフにします。

デバイスのセキュリティを確保するために、MAC アドレス学習機能をオフにする必要がある場合があります。デバイスのセキュリティが危険にさらされる一般的な状況は、不正なユーザが送信元 MAC アドレスが異なる大量のメッセージを使用してデバイスを攻撃し、デバイスの MAC アドレステーブルのリソースが枯渇し、デバイスがネットワークの変化に応じて MAC アドレステーブルを更新できなくなることです。MAC アドレス学習機能をオフにすると、この攻撃を効果的に防ぐことができます。

MAC アドレス学習機能をオフにする場合は、次の点に注意してください。

- MAC アドレス学習機能をオフにすると、デバイスは新しいアドレスを学習できなくなり、デバイスは MAC アドレステーブルを適時に更新できなくなります。ユーザは実際の状況に応じてインタフェースの MAC アドレス学習機能をオフにすることができる。
- グローバル MAC アドレス学習機能をオフにすると、インタフェースは新しい MAC アドレスを学習しなくなります。
- MAC アドレス学習機能をオフにするとブロードキャストが発生する可能性があるため、インタフェースの MAC アドレス学習機能をオフする場合は、事前にネットワークへの影響を考慮してください。
- グローバル MAC アドレス学習機能を有効にすると、デバイスの個々のインタフェースまたは指定した VLAN の MAC アドレス学習機能を無効にできます。
- MAC アドレス学習機能をオフにすると、すでに存在するダイナミック MAC アドレステーブルエントリは、エージングタイムがタイムアウトすると自然にエージングされます。

例

#グローバル MAC アドレス学習機能をオフにします。

<Sysname> system-view

[Sysname] undo mac-address mac-learning enable

#ポート GigabitEthernet1/0/1 の MAC アドレス学習機能をオフにします。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] undo mac-address mac-learning enable

#インタフェース Bridge-Aggregation1 の MAC アドレス学習機能をオフにします。

<Sysname> system-view

[Sysname] interface bridge-aggregation 1

[Sysname-Bridge-Aggregation1] undo mac-address mac-learning enable

関連コマンド

- display mac-address mac-learning

1.1.8 mac-address max-mac-count

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

デフォルト

インタフェースの MAC アドレス学習上限は 1024 である。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

count:インタフェースの MAC アドレス学習の上限値。0 は、インタフェースが MAC アドレスを学習できないことを示します。範囲は 0~1024 です。

説明

mac-address max-mac-count コマンドを使用して、インタフェースの MAC アドレス学習上限を設定します。

undo mac-address max-mac-count コマンドを使用して、デフォルトの状態を復元します。

インタフェースの MAC アドレス学習上限を設定することで、デバイスが保持する MAC アドレステーブルのエントリ数を制御できます。MAC アドレステーブルが大きすぎると、デバイスの転送パフォーマンスが低下する可能性があります。学習された MAC アドレスの数が上限に達すると、インタフェースは MAC アドレスを学習しなくなります。

例

#ポート GigabitEthernet1/0/1 の MAC アドレス学習の上限を 600 に設定します。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600

関連コマンド

- mac-address
- mac-address max-mac-count enable-forwarding (interface view)

1.1.9 mac-address max-mac-count enable-forwarding

Syntax

mac-address max-mac-count enable-forwarding

undo mac-address max-mac-count enable-forwarding

デフォルト

インタフェースの MAC アドレス学習上限に達すると、送信元 MAC アドレスが MAC アドレステーブルにないメッセージを転送できます。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-address max-mac-count enable-forwarding コマンドを使用して、インタフェースの MAC アドレス学習の上限に達したときに、送信元 MAC アドレスが MAC アドレステーブルにないメッセージを転送できるように設定します。

undo mac-address max-mac-count enable-forwarding コマンドは、インタフェースの MAC アドレス学習の上限に達した場合に、送信元 MAC アドレスが MAC アドレステーブルにないメッセージの転送を禁止するように設定します。

例

#ポート GigabitEthernet1/0/1 で学習される MAC アドレスの数の上限を 600 に設定し、ポートで学習される MAC アドレスの数が 600 時に達すると、送信元 MAC アドレスが MAC アドレステーブルにないメッセージの転送を禁止します。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600

[Sysname-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding

関連コマンド

- mac-address
- mac-address max-mac-count

1.1.10 mac-address notification mac-move

Syntax

mac-address notification mac-move [**interval** *interval*]

undo mac-address notification mac-move

デフォルト

MAC アドレス移行エスカレーション機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval *interval*:MAC アドレス遷移検出周期は、 1-60 の範囲で、単位は分である。このパラメータを指定しない場合、デフォルトの MAC アドレス移行検出サイクル 1 分が使用されます。

説明

mac-address notification mac-move コマンドは、MAC アドレス移行エスカレーション機能を有効にするために使用します。

undo mac-address notification mac-move コマンドは、MAC アドレス移行エスカレーション機能を無効にするために使用します。

MAC アドレス遷移のエスカレーション機能を起動した後、システムがアドレス遷移を検出した場合、MAC アドレス遷移検出周期の間隔によって前の MAC アドレス遷移検出周期内に発生した MAC アドレス遷移のログを記録し、MAC アドレス、その MAC アドレスが所在する VLAN ID、MAC アドレス遷移のソースインタフェースと新しいインタフェース、およびその MAC アドレスの MAC アドレス遷移検出周期内の遷移回数を含む。

1 回の MAC アドレス遷移検出周期で、最大 20 個の MAC アドレスの遷移ログを遷移回数の多い順に生成できる。この検出期間中に、新しく生成された移行ログの移行回数が、既存の移行ログの移行回数を超えると、移行回数が最も少ない移行ログは破棄され、新し

い移行ログは移行回数が多い順に並べられる。次の検出サイクルまで待つと、前の検出サイクルのすべてのログ情報が破棄され、移行ログの生成が再開されます。

本コマンドを実行した後、システムは Syslog 方式を採用して MAC アドレスの遷移情報を情報センターモジュールに報告し、もし同時に snmp-agent trap enable mac-address コマンドで MAC アドレス表の警報機能を起動すれば、システムは Trap 情報を採用して MAC アドレスの遷移情報を SNMP モジュールに報告する。

例

#MAC アドレス移行エスカレーション機能を有効にします。

<Sysname> system-view

[Sysname] mac-address notification mac-move

[Sysname]

```
%May 14 17:16:45:688 2013 Sysname MAC/4/MAC_FLAPPING:MAC address 0000-0012-
0034 in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times
```

上記の表示情報は、MAC アドレス 0000-0012-0034 が所在する VLAN ID が 500 であり、MAC アドレス遷移元インタフェースが GigabitEthernet1/0/1 であり、MAC アドレス遷移新インタフェースが GigabitEthernet1/0/2 であり、この MAC アドレスの 1 つの MAC アドレス遷移検出周期内の遷移回数が 1 であることを示す。

1.1.11 mac-address notification mac-move suppression (interface view)

Syntax

mac-address notification mac-move suppression

undo mac-address notification mac-move suppression

デフォルト

MAC アドレスの移行抑制機能がオフになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-address notification mac-move suppression コマンドを使用して、インタフェースで MAC アドレスの移行抑制機能を有効にします。

undo mac-address notification mac-move suppression コマンドを使用して、インタフェースの MAC アドレス移行抑制機能をオフにします。

MAC アドレス遷移抑制機能を起動した後、一つの MAC アドレス遷移検出周期内にある MAC アドレスがあるポートから遷移したまたはこのポートに遷移した回数が MAC アドレス遷移抑制の検出閾値を超えたことを監視すると、このポートを down し、ユーザはコマンド shutdown と undo shutdown を実行してこのポートを回復することができ、または MAC アドレス遷移抑制時間間隔を待ってからこのポートを自分で回復することができる。

MAC アドレス移行抑止機能によってポートがダウンすると、システムは情報センターモジュールにログ情報を送信し、デバイスが MAC アドレステーブルのアラーム機能(**snmp-agent trap enable mac-address** コマンド)をオンにしている場合は、デバイスの SNMP モジュールにアラーム情報を送信します。

例

#MAC アドレス移行抑制機能を有効にする。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] mac-address notification mac-move suppression

関連コマンド

- mac-address notification mac-move suppression (system view)

1.1.12 mac-address notification mac-move suppression (system view)

Syntax

mac-address notification mac-move suppression { **interval** *interval* | **threshold** *threshold* }

undo mac-address notification mac-move suppression { **interval** | **threshold** }

デフォルト

MAC アドレス遷移抑止機能に関連するパラメータは設定されておらず、デフォルトの抑止間隔は 30 秒、デフォルトのしきい値は 3 回です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval *interval*:MAC アドレス遷移抑止時間間隔(攻撃が検出された後、ポートがダウンしたままになるまでの時間)は、 30～86400 の範囲で秒単位で値をとる。このパラメータを指定しない場合、デフォルトの抑制間隔は 30 秒です。

threshold *threshold*:MAC アドレス遷移抑止の検出閾値(MAC アドレスの移行検出期間中に MAC アドレスの移行が許可される移行の最大数)、 0~1024 の範囲の値をとる。このパラメータを指定しない場合、デフォルトのしきい値が 3 回適用されます。

説明

mac-address notification mac-move suppression コマンドを使用して、MAC アドレス移行抑制機能の関連パラメータを設定します。

undo mac-address notification mac-move suppression コマンドを使用して、デフォルトの状態を復元します。

このコマンドで設定されたパラメータは、MAC アドレスの移行抑制機能がインタフェースでオンになっている場合にのみ有効になります。

このコマンドは複数回設定でき、interval interval と threshold threshold の設定には影響しません。

例

#MAC アドレス遷移抑止機能の抑止間隔を 40 s,検出閾値を 1 とする。

<Sysname> system-view

[Sysname] mac-address notification mac-move suppression interval 40

[Sysname] mac-address notification mac-move suppression threshold 1

関連コマンド

- mac-address notification mac-move suppression (interface view)

1.1.13 mac-address timer

Syntax

mac-address timer { **aging** *seconds* | **no-aging** }

undo mac-address timer

デフォルト

ダイナミック MAC アドレステーブルエントリのエージングタイムは 300 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

aging *seconds*:ダイナミック MAC アドレステーブルエントリのエージングタイム。秒単位で、値の範囲は 100~1400 です。

no-aging:老化しません。

説明

ダイナミック MAC アドレステーブルエントリのエージングタイムを設定するには、**mac-address timer** コマンドを使用します。

undo mac-address timer コマンドを使用して、デフォルトの状態を復元します。

ユーザ設定のエージングタイムが長すぎるか短すぎると、デバイスのパフォーマンスに影響する可能性があります。

- ユーザ設定のエージングタイムが長すぎると、デバイスが古い MAC アドレステーブルエントリを保持して MAC アドレステーブルリソースを使い果たし、ネットワークの変化に応じて MAC アドレステーブルを更新できなくなる可能性があります。
- ユーザが設定したエージングタイムが短すぎると、デバイスが有効な MAC アドレステーブルエントリを削除し、デバイスが大量のデータグラムをブロードキャストして、デバイスのパフォーマンスに影響を与える可能性があります。

したがってユーザは、 MAC アドレスエージング機能を効率的に実現するために、状況に応じて適切なエージング時間を設定する必要がある。

例

#ダイナミック MAC アドレステーブルエントリのエージングタイムを 500 秒に設定します。

<Sysname> system-view

[Sysname] mac-address timer aging 500

関連コマンド

- display mac-address aging-time

1.1.14 snmp-agent trap enable mac-address

Syntax

snmp-agent trap enable mac-address

undo snmp-agent trap enable mac-address

デフォルト

MAC アドレステーブルのアラーム機能がオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable mac-address コマンドを使用して、MAC アドレステーブルのアラーム機能をオンにします。

undo snmp-agent trap enable mac-address コマンドを使用して、MAC アドレステーブルのアラーム機能をオフにします。

MAC アドレステーブルのアラーム機能を有効にすると、MAC アドレステーブルモジュールは、モジュールの重要なイベントを報告するアラーム情報を生成します。生成されたアラーム情報はデバイスの SNMP モジュールに送信されます。SNMP のアラーム情報の送信パラメータを設定して、アラーム情報の出力に関する属性を決定します。

MAC アドレステーブルのアラーム機能をオフにすると、デバイスは情報センターモジュールにログ情報のみを送信します。この場合、情報センターの出力規則と出力方向を設定して、MAC アドレステーブルモジュールのログ情報を表示します。

SNMP の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

現在、MAC アドレステーブルモジュールは MAC アドレスマイグレーションのアラーム機能しか持っていないため、MAC アドレスマイグレーションのアラーム機能をオンまたはオフにすることは、MAC アドレステーブルのすべてのアラーム機能をオンまたはオフにすることに相当します。

例

#MAC アドレス移行のアラーム機能をオフにします。

<Sysname> system-view

[Sysname] undo snmp-agent trap enable mac-address

目次

このセクションのページは **5-x-x** です。

2 章 リンクアグリゲーション 2-1
2.1 リンクアグリゲーションコマンド 2-1
2.1.1 display interface 2-1
2.1.2 display link-aggregation load-sharing mode 2-5
2.1.3 display link-aggregation member-port 2-7
2.1.4 display link-aggregation summary 2-10
2.1.5 display link-aggregation verbose 2-11
2.1.6 interface bridge-aggregation 2-15
2.1.7 link-aggregation global load-sharing mode 2-16
2.1.8 link-aggregation load-sharing mode 2-17
2.1.9 link-aggregation selected-port maximum 2-18
2.1.10 link-aggregation mode 2-20
2.1.11 link-aggregation selected-port minimum 2-21
2.1.12 port link-aggregation group 2-22

2章 リンクアグリゲーション

2.1 リンクアグリゲーションコマンド

2.1.1 display interface

Syntax

display interface [**bridge-aggregation** [*interface-number*]] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation:レイヤ 2 集約インタフェースを指定します。

interface-number:既存の集約インタフェース番号を指定します。

brief:簡略的なインタフェース情報を表示します。このキーワードを指定しない場合、コマンドは詳細なインタフェース情報を表示します。

description:完全なインタフェースの説明を表示します。このキーワードを指定しない場合、各インタフェースの説明の最初の 27 文字だけが表示されます。

down:ダウン状態のインタフェースおよびダウン状態の原因に関する情報を表示します。このキーワードを指定しない場合、コマンドはすべての状態のインタフェースに関する情報を表示します。

説明

集約インタフェースタイプを指定しない場合、コマンドはすべてのインタフェースに関する情報を表示します。

集約インタフェースタイプを指定し、インタフェース番号を指定しない場合、コマンドは指定したタイプのすべての集約インタフェースに関する情報を表示します。

例

レイヤ 2 集約インタフェースの詳細情報を表示します。

<Sysname> display interface bridge-aggregation 1

```
Bridge-Aggregation1
```

```
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: 000f-e207-f2e0
Description: Bridge-Aggregation1 Interface
Bandwidth: 1000 kbps
2Gbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
PVID: 1
Port link-type: Access
 Tagged VLANs:   None
 UnTagged VLANs: 1
Last clearing of counters: Never
Last 300 seconds input:  6900 packets/sec 885160 bytes/sec    0%
Last 300 seconds output:  3150 packets/sec 404430 bytes/sec    0%
Input (total):  5364747 packets, 686688416 bytes
        2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input (normal):  5364747 packets, 686688416 bytes
        2682273 unicasts, 1341137 broadcasts, 1341337 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
        0 CRC, 0 frame, 0 overruns, - aborts
        - ignored, - parity errors
Output (total): 1042508 packets, 133441832 bytes
        1042306 unicasts, 0 broadcasts, 202 multicasts, - pauses
Output (normal): 1042508 packets, 133441832 bytes
        1042306 unicasts, 0 broadcasts, 202 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        - lost carrier, - no carrier
```

レイヤ 2 集約インタフェースの簡略情報を表示します。

<Sysname> display interface bridge-aggregation 1 brief

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) – auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface          Link Speed   Duplex Type PVID Description
BAGG1              DOWN auto    A      A    1
```

表 2-1　display interface コマンドの表示情報の説明

フィールド	説明

フィールド	説明
Bridge-Aggregation1	レイヤ2集約インタフェース名
Current state	物理インタフェースの状態： **Administratively DOWN**—shutdownコマンドによってshutdownされています。 **DOWN**—管理上はアップしていいますが、物理状態はダウンです（物理リンクが存在しないか、リンクに障害が発生している可能性があります）。 **UP**—インタフェースはアップしています。
IP packet frame type	IPv4パケットのフレームフォーマット
hardware address	インタフェースのMACアドレス
Description	インタフェースの説明
Bandwidth	インタフェースの予想帯域幅。帯域幅が0 kbpsの場合、このフィールドは表示されません。
Unknown-speed mode, unknown-duplex mode	インタフェース速度とデュプレックスモードは不明です。
PVID	インタフェースのPVID
Port link-type	ポートのリンクタイプ： **Access.** **Trunk.** **Hybrid.**
Tagged VLANs	パケットがタグ付きでこのインタフェースから送信されるVLAN
Untagged VLANs	パケットがタグなしでこのインタフェースから送信されるVLAN
Last clearing of counters	インタフェース統計情報をクリアするために**reset counters interface**コマンドが最後に使用された時刻。デバイスの起動後に**reset counters interface**コマンドがインタフェースで使用されたことがない場合、このフィールドには**Never**と表示されます。
Last 300 seconds input/output rate	過去300秒間の入力または出力の平均レート
Input/Output (total)	インタフェースで受信または送信されたすべてのパケットの統計情報
Input/Output (normal)	インタフェースで受信または送信されたすべての通常のパケットの統計情報
Line protocol state	インタフェースのデータリンクレイヤの状態 **UP**. **DOWN**.
Maximum transmission unit	MTUサイズ

フィールド	説明
Internet protocol processing	インタフェースにIPアドレスが割り当てられていない場合のインタフェースのIPパケット処理機能： **Disabled**—インタフェースはIPパケットを処理できません。 **Enabled**—インタフェースはIPパケットを処理できます。
Brief information on interfaces in bridge mode	簡略情報
Interface	省略されたインタフェース名
Link	インタフェースの物理リンク状態： **UP**—アップしています。 **DOWN**—ダウンしています。 **ADM**— **shutdown**コマンドを使用してインタフェースがシャットダウンされました。インタフェースの物理状態を復元するには、**undo shutdown**コマンドを使用します。 **Stby**—インタフェースはスタンバイステートのバックアップインタフェースです。
Speed	インタフェースの速度（bps単位）。 速度が自動的にネゴシエートされる場合、このフィールドには速度の横に（**a**）フラグが表示されます。 インタフェースが速度を自動ネゴシエーションするように設定されているが、自動ネゴシエーションが開始されていない場合、このフィールドには**auto**が表示されます。
Duplex	インタフェースのデュプレックスモード： **A(a)**— 自動ネゴシエーション。インタフェースはデュプレックスモードを自動ネゴシエーションするように設定されていますが、自動ネゴシエーションが開始されていません。 **F**—Full duplex. **H**—Half duplex.
Type	インタフェースのリンクタイプ： **A**—Access. **H**—Hybrid. **T**—Trunk.

フィールド	説明
Protocol	インタフェースのデータリンク層プロトコルの状態： **UP**—アップしています。 **DOWN**—ダウンしています。 **UP(s)**—インタフェースのデータリンク層プロトコルはアップしていますが、リンクはオンデマンドリンクであるか、存在しません。(s) 属性はスプーフィングフラグを表します。この値は、ヌルインタフェースおよびループバックインタフェースに一般的です。
Primary IP	インタフェースのプライマリIPアドレス。
Cause	インタフェースの物理リンク状態が**DOWN**になる原因。

2.1.2 display link-aggregation load-sharing mode

Syntax

display link-aggregation load-sharing mode interface [**bridge-aggregation** *interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation:レイヤ 2 集約インタフェースに対応する集約グループで使用される集約ロードシェアリングのタイプを表示します。

interface-number :集約インタフェースの番号。現在作成されている集約インタフェース番号である必要があります。

説明

display link-aggregation load-sharing mode コマンドを使用して、集約グループ内で使用されている集約の負荷分散タイプを表示します。

パラメータ interface が指定されていない場合は、グローバルに使用される集約ロードシェアリングタイプが表示されます。

特定の集約インタフェースタイプを指定せずにパラメータ interface のみを指定すると、すべての集約インタフェースに対応する集約グループで使用される集約負荷分散タイプが表示されます。

bridge-aggregation パラメータを指定できるのは、デバイスにレイヤ 2 集約インタフェースが作成されている場合だけです。

例

#グローバルに採用されている集約ロードシェアリングのタイプ(デフォルト)を表示します。

<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing algorithm:
4 (default)
Link-aggregation load-sharing seed:
0x1 (default)
Link-aggregation load-sharing mode:
Layer 2 traffic: destination-mac address　source-mac address
　　destination-ip address　　source-ip address

#グローバルに採用されている集約ロードシェアリングのタイプ(デフォルト以外の場合)を表示します。

<Sysname> display link-aggregation load-sharing mode
Link-aggregation load-sharing algorithm:
5
Link-aggregation load-sharing seed:
0 x 10
Link-aggregation load-sharing mode:
destination-mac addresssource-mac address

レイヤ 2 集約インタフェース 1 に対応する集約グループで使用される集約の負荷分散タイプ(デフォルト)を示します。

<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1
Layer 2 traffic:destination-mac addresssource-mac address
destination-ip addresssource-ip address

レイヤ 2 集約インタフェース 1 に対応する集約グループで使用される集約の負荷分散タイプ(デフォルト以外の場合)を示します。

<Sysname> display link-aggregation load-sharing mode interface bridge-aggregation 1
Bridge-Aggregation1 load-sharing mode:
destination-mac addresssource-mac address

表 2-2　display link-aggregation load-sharing mode コマンドの表示情報の説明

フィールド	説明
Link-aggregation load-sharing algorithm	グローバルに使用される集約負荷分散HASHアルゴリズム: • デフォルト:algorithm-number (default) • デフォルト以外で表示:ユーザ構成後に使用される集約負荷分散 HASH アルゴリズム
Link-aggregation load-sharing seed	グローバルに使用される統合された負荷分散HASH SEED • デフォルト:seed-number (default) • デフォルトで表示されない場合:ユーザ構成後の総負荷 HASH SEED
Bridge-Aggregation1 load-sharing mode	レイヤ2集約インタフェース1に対応する集約グループで使用される集約負荷分散のタイプ: • デフォルトの表示:グローバルに使用される集約ロードシェアリングタイプ • デフォルトで表示されない場合:ユーザ構成後に使用される集約ロードシェアリングタイプ
Layer 2 traffic:destination-mac addresssource-mac address destination-ip addresssource-ip address	デフォルトでは、送信元MACアドレス、宛先MACアドレス、宛先IPアドレス、および送信元IPアドレスに基づいて負荷を分散する、レイヤ2のメッセージの集約された負荷分散タイプが使用されます。
destination-mac address、source-mac address	ユーザ構成後の集約された負荷分散タイプ:送信元および宛先MACアドレス別の負荷分散

2.1.3 display link-aggregation member-port

Syntax

display link-aggregation member-port [*interface-list* | **auto**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-list:1 つ以上のメンバーポートを表すメンバーポートのリスト。interface-list =interface-type interface-number1 [to interface-type interface-number2]で表されます。ここで、interface-type はインタフェースタイプ、interface-number1 と interface-number2 はインタフェース番号です。interface-number2 の値は interface-number1 の値以上です。

auto:すべての自動集約メンバーポートのリンク集約の詳細を表示します。

説明

display link-aggregation member-port コマンドは、メンバーポートのリンク集約の詳細を表示します。

スタティックアグリゲーショングループはピア情報を認識できないため、スタティックアグリゲーショングループには、その側のポート番号、ポートプライオリティ、およびアクションキーの値のみが表示されます。

例

#静的集約グループ内のメンバーポート GigabitEthernet1/0/1 のリンク集約の詳細を表示します。

<Sysname> display link-aggregation member-port gigabitethernet 1/0/1
Flags:A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted、H -- Expired

GigabitEthernet1/0/1:
Aggregate Interface:Bridge-Aggregation1
Port Number:1
Port Priority:32768
Oper-Key:1

#動的集約グループ内のメンバーポート GigabitEthernet1/0/2 のリンク集約の詳細を表示します。

<Sysname> display link-aggregation member-port gigabitethernet 1/0/2
Flags:A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
D -- Synchronization, E -- Collecting, F -- Distributing,
G -- Defaulted、H -- Expired

GigabitEthernet1/0/2:
Aggregate Interface:Bridge-Aggregation10
Local:
Port Number:2
Port Priority:32768
Oper-Key:2
Flag:{ACDEF}

Remote:

System ID:0 x8000, 000 f-e267-6c6a

Port Number:26

Port Priority:32768

Oper-Key:2

Flag:{ACDEF}

Received LACP Packets:5 packet (s)

Illegal:0 packet (s)

Sent LACP Packets:7 packet (s)

表 2-3　display link-aggregation member-port コマンドの表示情報の説明

フィールド	説明
Flags	LACPプロトコルの状態標識は、長さが1バイトで、このバイトは下位から上位までそれぞれアルファベットのA~Hで表示し、ある一桁は1時に対応するアルファベットを印刷し、0時に対応するアルファベットを印刷しない。各フラグの意味は次のとおりです。 • A:LACP オンフラグかどうか。1 はオン;0 はオフ • B:LACP Long/Short Timeout フラグ。1 は短いタイムアウト;0:長いタイムアウト • C:送信側は、このメンバーポートが存在するリンクが集約可能かどうかを判断する。1 は Yes を表します;0 は No を表します • D:送信側は、このメンバーポートが存在するリンクが同期状態にあるかどうかを判断する。1 は Yes を表します;0 は No を表します • E:送信側は、このメンバーポートが存在するリンクが収集状態であるかどうかを判断する。1 は Yes を表します;0 は No を表します • F:送信側は、このメンバーポートが存在するリンクが配布されているかどうかを認識する。1 は Yes を表します;0 は No を表します • G:送信側の受信状態マシンがデフォルト状態かどうか。1 は Yes を表します;0 は No を表します • H:送信側の受信状態マシンがタイムアウト状態かどうか。1 は Yes を表します;0 は No を表します
Aggregate Interface	このメンバーポートが属する集約インタフェース
Preferred Aggregate Interface	半自動アグリゲーション参加するアグリゲーションの優先順位
Local	ローカル情報
Port Number	ポート番号
Port Priority	ポートプライオリティ

フィールド	説明
Oper-key	アクションKeyの値
フラッグ	LACPプロトコルのステータスフラグ値
Remote	ピア情報
System ID	デバイスID (システムのLACPプライオリティとシステムのMACアドレスから構成される.)
Received LACP Packets	受信したLACPメッセージの合計数
Illegal	不正メッセージの総数
Sent LACP Packets	発行されたLACPメッセージの合計数

2.1.4 display link-aggregation summary

Syntax

display link-aggregation summary

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display link-aggregation summary コマンドは、すべての集約グループのサマリー情報を表示します。

スタティックアグリゲーショングループはピア情報を認識できないため、スタティックアグリゲーショングループのピア情報は None と表示され、ピアシステムの実際の情報を表しません。

例

#すべての集約グループの要約情報を表示します。

<Sysname> display link-aggregation summary

Aggregate Interface Type:

BAGG -- Bridge-Aggregation, BLAGG –- Blade-Aggregation, RAGG -- Route-Aggregatio

n, SCH-B – Schannel-Bundle

Aggregation Mode: S -- Static, D -- Dynamic

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Actor System ID: 0x8000, 000f-e267-6c6a

AGG　　AGG　Partner ID　　Selected　Unselected　Individual　Share

```
Interface    Mode                          Ports      Ports      Ports      Type
--------------------------------------------------------------------------------
BAGG20       D       0x8000,00e0-fcff-ff01 2          0          0          Shar
```

表 2-4　display link-aggregation summary コマンドの表示情報の説明

フィールド	説明
Aggregate Interface Type	集約インタフェースのタイプ: • BAGG:レイヤ 2 集約インタフェースを表します。
Aggregation Mode	集約グループ・タイプ: • S:静的集約の場合 • D:動的集約の場合
Loadsharing Type	負荷分散のタイプ: • Shar:負荷分散タイプを表します。 • NonS:非負荷分散タイプを表します。
Actor System ID	ローカル側のデバイスID (システムのLACPプライオリティとシステムのMACアドレスから構成される.)
AGG Interface	集約インタフェースのタイプと数
AGG Mode	集約グループのタイプ
Partner ID	ピアのデバイスID (システムのLACPプライオリティとシステムのMACアドレスから構成される.)
Selected Ports	選択したメンバーポートの数
Unselected Ports	選択されていないメンバーポートの数
Individual Ports	スタンドアロン状態のメンバーポートの数
Share Type	負荷分散タイプ

2.1.5 display link-aggregation verbose

Syntax

display link-aggregation verbose [**bridge-aggregation** [*interface-number*]] [**all-configuration**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

bridge-aggregation:レイヤ 2 集約インタフェースに対応する集約グループの詳細を表示します。

interface-number:集約インタフェースの番号。現在作成されている集約インタフェース番号である必要があります。

all-configuration:集約グループ内のすべてのメンバーポートが表示されます。このパラメータが指定されていない場合は、集約グループ内のビット・シングル・ボード上のメンバーポートが表示されます。

説明

display link-aggregation verbose コマンドは、既存の集約インタフェースに対応する集約グループの詳細を表示します。

集約インタフェースのタイプを指定しない場合は、デバイスがサポートするすべてのインタフェースに関する情報が表示されます。

集約インタフェースのタイプのみを指定した場合は、作成されたそのタイプのすべての集約インタフェースに関する情報が表示されます。

bridge-aggregation パラメータを指定できるのは、デバイスにレイヤ 2 集約インタフェースが作成されている場合だけです。

集約グループに実際に参加していない自動集約ポートは表示されません。

例

#レイヤ 2 集約インタフェース 10 に対応する集約グループは、動的集約グループであり、その集約グループの詳細を表示する。

```
<Sysname> display link-aggregation verbose bridge-aggregation 10
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Role: P -- Primary, S -- Secondary

Aggregate Interface: Bridge-Aggregation10
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port            Status  Priority Index   Oper-Key          Flag
  GE1/0/1         S       32768    61      2                 {ACDEF}
```

```
  GE1/0/2          S       32768   62      2                   {ACDEF}
  GE1/0/3          S       32768   63      2                   {ACDEF}
Remote:
  Actor            Priority Index   Oper-Key SystemID                Flag
  GE1/0/1(R)       32768    111     2        0x8000, 000f-e267-57ad  {ACDEF}
  GE1/0/2          32768    112     2        0x8000, 000f-e267-57ad  {ACDEF}
  GE1/0/3          32768    113     2        0x8000, 000f-e267-57ad  {ACDEF}
```

#レイヤ 2 集約インタフェース 20 に対応する集約グループは、静的集約グループであり、その集約グループの詳細を表示する。

```
<Sysname> display link-aggregation verbose bridge-aggregation 20
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired
Role: P -- Primary, S -- Secondary

Aggregate Interface: Bridge-Aggregation20
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority Oper-Key  Role
  GE1/0/1(R)       S       32768    1         None
  GE1/0/2          S       32768    1         None
  GE1/0/3          S       32768    1         None
```

表 2-5　display link-aggregation verbose コマンドの表示情報の説明

フィールド	説明
Loadsharing Type	負荷分散のタイプ: • Shar:負荷分散タイプを表します。 • NonS:非負荷分散タイプを表します。
Port Status	ポートの状態: • Selected:が選択されていることを示します。 • Unselected:選択されていないことを示します。 • Individual:スタンドアロン状態であることを示します。

フィールド	説明
Port	ポートタイプ: • Auto port:ポートが自動ポートであることを示します。 • Management port:ポートが管理ポートであることを示します。 • Reference port:ポートが参照ポートであることを示します。
Flags	LACPプロトコルの状態フラグは、長さが1バイトであり、そのバイトは下位から上位までそれぞれアルファベットのA¯Hで表され、値が1をとるフラグは対応するアルファベットで表示され、値が0をとるフラグは表示されない。各フラグの意味は次のとおりです。 • A:LACP オンフラグかどうか。1 はオン;0 はオフ • B:LACP Long/Short Timeout フラグ。1 は短いタイムアウト;0:長いタイムアウト • C:送信側は、このメンバーポートが存在するリンクが集約可能かどうかを判断する。1 は Yes を表します;0 は No を表します • D:送信側は、このメンバーポートが存在するリンクが同期状態にあるかどうかを判断する。1 は Yes を表します;0 は No を表します • E:送信側は、このメンバーポートが存在するリンクが収集状態であるかどうかを判断する。1 は Yes を表します;0 は No を表します • F:送信側は、このメンバーポートが存在するリンクが配布されているかどうかを認識する。1 は Yes を表します;0 は No を表します • G:送信側の受信状態マシンがデフォルト状態かどうか。1 は Yes を表します;0 は No を表します • H:送信側の受信状態マシンがタイムアウト状態かどうか。1 は Yes を表します;0 は No を表します
Role	(未サポート) 1:1プライマリバックアップモード集約グループのメンバーインタフェースの役割: • Primary:プライマリインタフェース • Secondary:バックアップインタフェース 構成されていない集約グループが1:1プライマリバックアップモードでNoneとして動作している
Aggregate Interface	集約インタフェースの名前

フィールド	説明
Creation Mode	動的集約グループの作成方法: • Auto:自動作成を表します。 • Manual:手動で作成されたことを示します。
Aggregation Mode	集約グループの動作モード: • Static:静的集約の場合 • Dynamic:動的集約の場合
Management VLANs	管理VLAN、指定されていない場合はNone
System ID	デバイスID (システムのLACPプライオリティとシステムのMACアドレスから構成される.)
Local	ローカル情報: • Port:ポートのタイプと番号 • Status:ポートが選択されている/選択されていない/スタンドアロン状態 • Priority:ポートプライオリティ • Index:ポートインデックス • Oper-Key:アクション Key の値 • Flag:LACP プロトコルのステータスフラグ値 🕮 メモ : 静的な集計グループはローカル情報のみを表示し、Index および Flag フィールドは表示されません。
Remote	ピア情報: • Actor:ピアポートが参照ポートの場合は、そのポートのタイプと番号が、対応するピアポートに表示されます。 • Priority:ピアポートのポートプライオリティ • Index:ピアポートのポートインデックス • Oper-Key:エンドポートに対するアクション Key の値 • System ID:ピアのデバイス ID • Flag:ピアの LACP プロトコルのステータスフラグ値

2.1.6 interface bridge-aggregation

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

デフォルト

レイヤ 2 集約インタフェースはありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number:レイヤ 2 集約インタフェースの番号を 1~4 の範囲で指定します。

説明

interface bridge-aggregation コマンドを使用して、レイヤ 2 集約インタフェースを作成し、Layer 2 aggregate interface view に入ります。指定したレイヤ 2 集約インタフェースがすでに存在する場合は、その Layer 2 aggregate interface view に直接移動します。

undo interface bridge-aggregation コマンドは、レイヤ 2 集約インタフェースを削除するために使用します。

レイヤ 2 集約インタフェースを作成すると、同じ番号のレイヤ 2 集約グループが自動的に生成され、デフォルトでは静的集約モードで動作します。

レイヤ 2 集約インタフェースを削除すると、対応するレイヤ 2 集約グループも削除されます。集約グループ内にメンバーポートがある場合、メンバーポートは自動的に集約グループから削除されます。

例

レイヤ 2 集約インタフェース 1 を作成しその view に進みます。

<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1]

2.1.7 link-aggregation global load-sharing mode

Syntax

link-aggregation global load-sharing mode { **destination-ip** | **destination-mac** | **destination-port** | **source-ip** | **source-mac** | **source-port** }

undo link-aggregation global load-sharing mode

デフォルト

デバイスは、送信元 MAC アドレス、宛先 MAC アドレス、送信元 IP アドレス、および宛先 IP アドレスに基づいてロードシェアリングを集約します。

View

System view

定義済みユーザロール

network-admin

パラメータ

destination-ip:メッセージの宛先 IP アドレスによる集約負荷分散を示す。

destination-mac:メッセージの宛先 MAC アドレスごとに集約負荷分散を行うことを示す。

destination-port:メッセージの宛先サービスポートごとに負荷を分散することを示す。

source-ip:メッセージの送信元 IP アドレスによる集約負荷分散を示す。

source-mac:メッセージの送信元 MAC アドレスによる集約負荷分散を示す。

source-port:メッセージの送信元サービスポートごとに負荷を分散することを示す。

説明

link-aggregation global load-sharing mode コマンドを使用して、グローバルに使用される集約ロードシェアリングタイプを設定します。

undo link-aggregation global load-sharing mode コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

デバイスでサポートされていない集約型の負荷分散タイプについては、サポートされていないことを示すメッセージが表示されます。

例

#メッセージの宛先 MAC アドレスごとに集約されたロードシェアリングをグローバルに設定します。

<Sysname> system-view
[Sysname] link-aggregation global load-sharing mode destination-mac

関連コマンド

- **link-aggregation load-sharing mode**

2.1.8 link-aggregation load-sharing mode

Syntax

link-aggregation load-sharing mode { **destination-ip** | **destination-mac** | **source-ip** | **source-mac** } *

undo link-aggregation load-sharing mode

デフォルト

集約グループ内で使用される集約負荷分散タイプは、グローバルで使用される集約負荷分散タイプと一致します。

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

destination-ip:メッセージの宛先 IP アドレスによる集約負荷分散を示す。

destination-mac:メッセージの宛先 MAC アドレスごとに集約負荷分散を行うことを示す。

source-ip:メッセージの送信元 IP アドレスによる集約負荷分散を示す。

source-mac:メッセージの送信元 MAC アドレスによる集約負荷分散を示す。

説明

link-aggregation load-sharing mode コマンドを使用して、集約グループ内で使用される集約の負荷分散タイプを設定します。

undo link-aggregation load-sharing mode コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

デバイスでサポートされていない集約型の負荷分散タイプについては、サポートされていないことを示すメッセージが表示されます。

例

#レイヤ 2 集約インタフェース 1 に対応するアグリゲーショングループ内でメッセージ先 MAC アドレスによる負荷分散を設定する。

<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation load-sharing mode destination-mac

関連コマンド

- **link-aggregation global load-sharing mode**

2.1.9 link-aggregation selected-port maximum

Syntax

link-aggregation selected-port maximum *max-number* [**lacp-sync**]

undo link-aggregation selected-port maximum

デフォルト

アグリゲーショングループ内の最大値は 16 です。

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

max-number:集約グループ内の最大総ポート数。範囲は 1~16 です。

lacp-sync:LACPDU を使用してポートの最大数を同期するように動的集約グループを構成し、両端の集約グループの最大数のポートを一致させます。このパラメータが指定されていない場合、最大値のポート数は同期されません。

説明

link-aggregation selected-port maximum コマンドを使用して、集約グループ内のポートの最大数を設定します。

undo link-aggregation selected-port maximum コマンドを使用して、デフォルトの状態を復元します。

このコマンドを実行すると、集約グループ内のメンバーポートの一部が選択解除される場合があります。

静的な集約グループの場合、この側と反対側で構成された集約グループ内の最大ポート数は一致している必要があります。動的集約グループの場合、lacp-sync パラメータを指定しないと、ローカル側とピア側で構成された集約グループ内の最大ポート数が一致する必要があります。lacp-sync パラメータが指定されている場合、ローカルおよびピアアグリゲーショングループ内の最大のポート数は、構成されている値の最も小さい側になります。

同じ集約グループ内で、選択されているポート数の最小構成値を下回ることはできません。

集約グループ内のポートの最大数を構成すると、最大数は構成値とデバイスのハードウェア機能の両方によって制限されます。つまり、両方の値のうち小さい方が制限値として使用されます。

これにより、1 つの集約グループに 2 つのメンバーポートのみを追加し、集約グループ内の最大ポート数を 1 に設定することで、2 つのメンバーポートのうち 1 つだけが同時に選択され、もう 1 つはバックアップ・ポートとして使用されるように、2 つのポート間で冗長バックアップを実行できます。

例

#レイヤ 2 集約インタフェースの設定 1 対応する集約グループの最大値はポート数 5 です。

<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port maximum 5

関連コマンド

- **link-aggregation selected-port minimum**

2.1.10 link-aggregation mode

Syntax

link-aggregation mode { **dynamic** | **static**}

undo link-aggregation mode

デフォルト

アグリゲーショングループはスタティックアグリゲーションモードで動作します。

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

dynamic：動的モードを指定し、LACP を有効にします。

static：静的モードを指定します。

説明

link-aggregation mode コマンドを使用して、アグリゲーショングループの集約モードを設定します。

undo link-aggregation mode コマンドを使用して、デフォルトに戻します。

アグリゲーションモードを変更する際は、変更がサービスに与える影響を十分に理解してください。

アグリゲーションモードの変更により、選択済みメンバーポートが未選択になる場合があります。

例

#レイヤ 2 アグリゲーショングループ 1 を動的モードで動作するように設定します。

<Sysname> system-view

[Sysname] interface bridge-aggregation
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic

2.1.11 link-aggregation selected-port minimum

Syntax

link-aggregation selected-port minimum *min-number*

undo link-aggregation selected-port minimum

デフォルト

集約グループで選択されているポートの最小数に制限はありません。

View

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

min-number:選択した集約グループ内のポートの最小数。範囲は 1~16 です。

説明

link-aggregation selected-port minimum コマンドを使用して、集約グループ内の選択したポートの最小数を設定します。

undo link-aggregation selected-port minimum コマンドを使用して、デフォルトの状態を復元します。

このコマンドを実行すると、集約グループ内のすべてのメンバーポートが選択解除される場合があります。

選択されたポートの最小数は、ローカルとピアで構成された集約グループ内で一致している必要があります。

同じ集約グループ内で、選択された最小ポート数構成値は、選択された最大ポート数構成値より大きくすることはできません。

例

#レイヤ 2 集約インタフェースの設定 1 対応する集約グループの最小選択ポート数は 3 です。

<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation selected-port minimum 3

関連コマンド

- **link-aggregation selected-port maximum**

2.1.12 port link-aggregation group

Syntax

port link-aggregation group { *group-id* [**force**] | **auto** [*group-id*] }

undo port link-aggregation group

デフォルト

イーサネットインタフェースは集約グループに参加していません。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

group-id:集約グループに対応する集約インタフェースの番号を 1~4 の範囲で指定します。

force:インタフェースがアグリゲーショングループに参加したときに、そのアグリゲーショングループの属性クラス設定を同期することを示します。このパラメータを指定しない場合は、インタフェースが集約グループに参加したときに、その集約グループの属性クラス構成が同期されないことを示します。このパラメータの指定は、レイヤ 2 イーサネットインタフェースでのみサポートされています。

auto:自動集約機能をオンにします。

説明

port link-aggregation group コマンドを使用して、指定した集約グループにインタフェースを結合します。

undo port link-aggregation group コマンドは、結合された集約グループからインタフェースを削除するために使用します。

レイヤ 2 イーサネットインタフェースは、レイヤ 2 集約グループにのみ割り当てることができます。

インタフェースは、1 つの集約グループにのみ属することができます。

集約インタフェースと異なる属性設定を持つインタフェースは、集約グループに参加できません。集約グループに参加した後、インタフェースは集約インタフェースの属性設定を継承します。集約インタフェースでのみ属性設定を変更できます。

force キーワードは、インタフェースを集約グループに割り当てた場合にのみ有効になります。実行コンフィギュレーションまたはコンフィギュレーションファイルに保存することはできません。

自動割り当てを有効にすると、優先集約グループを指定できます。このグループはダイナミックモードである必要があります。

インタフェースで受信したLACPDUがグループ内のリファレンスポートのピア情報と一致する限り、デバイスはインタフェースを優先集約グループに割り当てます。

優先グループを指定しない場合、または優先グループの一致に失敗した場合、デバイスは既存の動的集約グループから一致するグループを選択しようとします。一致が見つからない場合、デバイスはLACPDUに基づいて動的集約グループを作成し、その集約グループにインタフェースを割り当てます。

ベストプラクティスとして、自動的に作成された集約インタフェースまたはそのメンバーポートの設定を変更しないでください。

例

#レイヤ 2 イーサネットインタフェース GigabitEthernet1/0/1 をレイヤ 2 アグリゲーショングループ 1 に追加します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-aggregation group 1
```

目次

このセクションのページは **5-x-x** です。

3 章 VLAN 3-1
3.1 VLAN 設定コマンド 3-1
3.1.1 description 3-1
3.1.2 display interface vlan-interface 3-2
3.1.3 display vlan 3-5
3.1.4 display vlan brief 3-7
3.1.5 interface vlan-interface 3-8
3.1.6 name 3-9
3.1.7 shutdown 3-10
3.1.8 vlan 3-11
3.2 ポートベースの VLAN 設定コマンド 3-13
3.2.1 display port 3-13
3.2.2 port 3-14
3.2.3 port access vlan 3-15
3.2.4 port hybrid pvid 3-16
3.2.5 port hybrid vlan 3-17
3.2.6 port link-type 3-18
3.2.7 port trunk permit vlan 3-19
3.2.8 port trunk pvid 3-20

3章 VLAN

3.1 VLAN設定コマンド

3.1.1 description

Syntax

description *text*

undo description

デフォルト

VLAN *vlan-id* です。*vlan-id* 引数は、4 桁の形式で VLAN ID を指定します。VLAN ID が 4 桁未満の場合は、先頭に 0 が追加されます。たとえば、VLAN 100 のデフォルトの説明は VLAN 0100 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

text:説明を指定します。1 文字以上 255 文字以下で、大文字と小文字が区別されます。

説明

Description コマンドを使用して、VLAN の説明を設定します。

undo description コマンドを使用して、デフォルトに戻します。

VLAN を効率的に管理するには、機能または接続情報に基づいた説明を設定します。

例

VLAN 2 の説明を **sales-private** に設定します。
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] description sales-private

関連コマンド

- **display vlan**

3.1.2 display interface vlan-interface

Syntax

display interface [**vlan-interface** [*interface-number*]] [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-interface *interface-number*:指定した VLAN インタフェースの情報を表示する VLAN インタフェースの番号。vlan-interface パラメータを指定しない場合、デバイスがサポートするすべてのインタフェースに関する情報が表示されます。vlan-interface パラメータを指定し、interface-number パラメータを指定しない場合、作成されたすべての VLAN インタフェースの情報が表示されます。

brief:インタフェースのサマリー情報を表示します。このパラメータを指定しない場合、インタフェースの詳細が表示されます。

説明

display interface vlan-interface コマンドを使用して、VLAN インタフェースに関する情報を表示します。

例

#VLAN-interface 2 に関する情報を表示します。

<Sysname> display interface vlan-interface 2
Vlan-interface2
Current state: DOWN
Line protocol state: DOWN
Description: Vlan-interface2 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1500
Internet protocol processing : Disabled
IP packet frame type: Ethernet II, hardware address: 000f-e249-8050
IPv6 packet frame type: Ethernet II, hardware address: 000f-e249-8050
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops

#VLAN-interface 2 のサマリー情報を表示します。

<Sysname> display interface vlan-interface 2 brief

Brief information on interfaces in route mode:

Link: ADM - administratively down; Stby - standby

Protocol: (s) - spoofing

Interface Link Protocol Primary IP Description

Vlan2 DOWN DOWN --

表 3-1 display interface vlan-interface コマンドの表示情報の説明

フィールド	説明
Vlan-interface2	VLANインタフェース名
Current state	VLANインタフェースの物理状態。状態は次のとおりです。 • Administratively DOWN:VLAN インタフェースが shutdown コマンドでシャットダウンされたことを示します。つまり、管理状態はシャットダウンです。 • DOWN:その VLAN インタフェースの管理状態は ON であるが、物理状態は OFF であることを示します。つまり、そのインタフェースに対応する VLAN 内に UP 状態の物理ポートがないことを示します(物理的な接続がないか、回線が故障している可能性があります)。 • UP:このポートの管理状態と物理状態の両方がオンです。
Line protocol state	VLANインタフェースのリンク層プロトコルの状態。 • DOWN:この VLAN インタフェースのプロトコルステータスはオフです • UP:この VLAN インタフェースのプロトコルステータスはオンです
Description	VLANインタフェースの説明
Bandwidth	VLANインタフェースの予想帯域幅
Maximum transmission unit	VLANインタフェースで許可されるMTU
Internet protocol processing	インタフェースにIPアドレスが設定されていません。インタフェースのネットワークプロトコル設定パラメータ: • Disabled:IP メッセージを処理できません • Enabled:IP メッセージを処理できます。
IP packet frame type	IPv 4送信フレームフォーマット
hardware address	VLANインタフェースに対応するMACアドレス
IPv6 packet frame type	IPv 6送信フレームフォーマット

フィールド	説明
Last clearing of counters	最後にreset counters interface vlan-interfaceコマンドを使用してインタフェースから統計情報をクリアした時刻。デバイスからの起動時にreset counters interface vlan-interfaceコマンドを実行せずにインタフェースの統計情報をクリアした場合は、Neverと表示されます。
Last 300 seconds input rate:0 bytes/sec, 0 bits/sec, 0 packets/sec Last 300 seconds output rate:0 bytes/sec, 0 bits/sec, 0 packets/sec	現在のインタフェースの過去300秒間の入力(input)および出力(output)メッセージの平均レート(単位は、バイト/秒、ビット/秒、パケット/秒である。)。
Input:0 packets, 0 bytes, 0 drops	インタフェースで入力されたメッセージの総数(それぞれパケットとバイト単位で統計をとった)。入力メッセージでドロップされたメッセージの数。
Output:0 packets, 0 bytes, 0 drops	インタフェースから出力されたメッセージの総数(それぞれパケットとバイト単位で統計をとった)、出力メッセージでドロップされたメッセージの数。
Brief information on interfaces in route mode	3層モード(route)のインタフェースのサマリー情報、つまり3層インタフェースのサマリー情報
リンク:ADM - administratively down;Stby - standby	• インタフェースの Link プロパティの値が「ADM」の場合、そのインタフェースは shutdown コマンドによって管理者によってシャットダウンされ、ポート自体の物理状態を復元するには、そのインタフェースで undo shutdown コマンドを実行する必要があります。 • インタフェースの Link プロパティの値が「スティビー」の場合は、そのインタフェースが Standby のバックアップインタフェースであり、display interface-backup state コマンドを使用してそのバックアップインタフェースのプライマリ・インタフェースを表示します。
Protocol: (s) -spoofing	インタフェースのProtocol属性値に「(s)」文字列が含まれている場合は、そのインタフェースのデータリンク層プロトコルステータスがUPと表示されますが、実際には対応するリンクが存在しないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があります。
Interface	インタフェース名の省略名

フィールド	説明
Link	インタフェースの物理接続ステータス。次の値をとります。 • UP:インタフェースが物理的に接続されていることを示します。 • DOWN:インタフェースが物理的に接続されていないことを示します • ADM:管理者が shutdown コマンドを使用してインタフェースをシャットダウンしたことを示します。インタフェース自体の物理状態を回復するには、undo shutdown コマンドを実行する必要があります。 • Stby:インタフェースが状態 Standby のバックアップインタフェースであることを示します。
Protocol	インタフェースデータリンク層プロトコルの状態。次の値を取ります。 • UP:インタフェースのデータリンク層プロトコルステータスがオンであることを示します。 • DOWN:インタフェースのデータリンク層プロトコルの状態がオフであることを示します • UP (s) :インタフェースのデータリンク層プロトコルステータスが UP と表示されているが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があります。
Primary IP	インタフェースのプライマリIPアドレス

関連コマンド

- **reset counters interface vlan-interface**

3.1.3 display vlan

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id1:指定した VLAN の情報を表示します。vlan-id1 は VLAN の番号で、範囲は 1~4094 です。

vlan-id1 **to** *vlan-id2*:ID が指定された範囲内にある VLAN の情報を表示します。vlan-id1 と vlan-id2 は指定された VLAN の番号で、値の範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。

all:予約済み VLAN 以外の VLAN の情報を表示します。

dynamic:システムが動的に作成する VLAN の数と数を表示します。

reserved:システムが予約している VLAN に関する情報を表示します。予約済み VLAN は、機能の実装に応じてデバイスが予約する VLAN です。予約済み VLAN はプロトコルモジュールによって指定され、プロトコルモジュールにサービスを提供します。予約済み VLAN に対してユーザは何もできません。

static:システムがスタティックに作成した VLAN の数と VLAN 番号を表示します。スタティック VLAN は、コマンドラインを使用して手動で作成された VLAN です。

説明

display vlan コマンドを使用して、VLAN に関する情報を表示します。

例

#VLAN 2 の情報を表示します。

```
<Sysname> display vlan 2
 VLAN ID: 2
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:     None
 Untagged ports:
    GigabitEthernet1/0/1    GigabitEthernet1/0/2    GigabitEthernet1/0/3
```

#VLAN 3 の情報を表示します。

```
<Sysname> display vlan 3
 VLAN ID: 3
 VLAN type: static
 Route interface: Configured
 IPv4 address: 1.1.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged ports:     None
 Untagged ports: None
```

表 3-2 display vlan コマンドの表示情報の説明

フィールド	解釈
VLAN ID	VLANの番号
VLAN type	VLANのタイプ: • Static:スタティック VLAN • Dynamic:ダイナミック VLAN
Route interface	対応するVLANインタフェースがデバイスに作成されているかどうか。 • Not configured:作成されていません • Configured:作成済み
Description	VLANの説明
Name	VLANの名前
IP address	VLANインタフェースのプライマリIPアドレス。VLANインタフェースにIPアドレスが設定されていない場合は表示されません。VLANインタフェースにスレーブIPアドレスも設定されている場合は、display interface vlan-interfaceを使用するか、VLAN interface viewでdisplay thisコマンドを使用して表示できます。
Subnet mask	VLANインタフェースのプライマリIPアドレスのサブネットマスク。VLANインタフェースにIPアドレスが設定されていない場合は表示されません。
Tagged ports	このVLANメッセージをどのポートから送信する場合にTagタグが必要か
Untagged ports	このVLANメッセージが送信されるポートにTagタグを付ける必要はありません。

関連コマンド

- **vlan**

3.1.4 display vlan brief

Syntax

display vlan brief

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display vlan brief コマンドは、デバイスで作成されたすべての VLAN のサマリー情報を表示します。

例

#デバイスで作成されたすべての VLAN のサマリー情報を表示します。

<Sysname> display vlan brief
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID Name Port
1 VLAN 0001 GE1/0/1 GE1/0/2 GE1/0/3 GE1/0/4
GE1/0/5 GE1/0/6 GE1/0/7 GE1/0/8
2 VLAN 0002
3 VLAN 0003

表 3-3 display vlan brief コマンドの表示情報の説明

フィールド	説明
Brief information about all VLANs:	すべてのVLANのプロファイル
Supported Minimum VLAN ID	システムでサポートされている最小値VLAN ID
Supported Maximum VLAN ID	システムでサポートされている最大VLAN ID
Default VLAN ID	デフォルトVLAN ID
VLAN ID	VLANの番号
Name	VLANの名前
Port	このVLANメッセージが通過できるポート

3.1.5 interface vlan-interface

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

デフォルト

VLAN インタフェースがありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number :VLAN インタフェースの番号。範囲は 1~4094 です。

説明

interface vlan-interface コマンドを使用して、VLAN インタフェースを作成し、VLAN interface view にアクセスします。VLAN インタフェースがすでに存在する場合は、VLAN interface view に直接進みます。

undo interface vlan-interface コマンドを使用して、指定した VLAN インタフェースを削除します。

VLAN インタフェースを作成する前に、対応する VLAN がすでに存在している必要があります。存在していない場合は、指定した VLAN インタフェースを作成できません。

Sub VLAN 対応する VLAN インタフェースを作成できません。

レイヤ 3 インターワーキングが Primary VLAN interface で設定されている Secondary VLAN は、対応する VLAN インタフェースを作成できません。

例

#VLAN インタフェース 2 を作成し、view に移動します。

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]

関連コマンド

- **display interface vlan-interface**

3.1.6 name

Syntax

name *text*

undo name

デフォルト

VLAN の名前は「VLAN vlan-id」です。ここで、vlan-id は VLAN の 4 桁の番号です。VLAN の番号が 4 桁未満の場合は、番号の前に 0 が付加され、4 桁が補われます。たとえば、VLAN 100 の名前は「VLAN 0100」です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

text:1~32 文字の VLAN 名で、大文字と小文字が区別されます。

説明

name コマンドは、現在の VLAN の名前を指定します。

undo name コマンドを使用して、デフォルトの状態を復元します。

VLAN の数が多い場合は、名前を使用して VLAN をより明確に特定できます。

例

#VLAN 2 の名前を「test vlan」に指定します。

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] name test vlan

関連コマンド

- **display vlan**

3.1.7 shutdown

Syntax

shutdown

undo shutdown

デフォルト

VLAN インタフェースはダウン状態です。

View

VLAN interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドは、VLAN インタフェースを手動でシャットダウンするために使用されます。

undo shutdown コマンドは、VLAN インタフェースを手動で開くために使用されます。

注意

このコマンドを実行すると、その VLAN インタフェースを使用して確立されたリンクがダウンし、通信できなくなる可能性があるため、注意して使用してください。

VLAN インタフェースを手動でシャットダウンしなかった場合、VLAN インタフェースの状態は、VLAN 内のポートの状態によって影響を受けます。

- VLAN 内のすべてのイーサネットポートの状態が down の場合、VLAN インタフェースは down、つまりダウン状態になります。
- VLAN 内の 1 つ以上のイーサネットポートが up 状態の場合、VLAN インタフェースは up 状態になります。

VLAN インタフェースを手動でシャットダウンすると、VLAN インタフェースの状態は常に down (Administratively)になり、VLAN 内のポートの状態には影響されません。

VLAN インタフェースパラメータを設定する前に、設定中のネットワークへの影響を避けるために、パラメータを設定する前に shutdown コマンドを使用してインタフェースを手動でシャットダウンすることをお勧めします。設定が完了したら、undo shutdown コマンドを使用してインタフェースの手動シャットダウンを解除し、設定したパラメータを有効にします。

VLAN インタフェースに障害が発生した場合は、shutdown コマンドを使用してインタフェースを手動でシャットダウンし、undo shutdown コマンドを使用してインタフェースの手動シャットダウンを解除することで、インタフェースを正常に戻すことができます。

VLAN インタフェースのシャットダウンとオープンは、その VLAN に属する Ethernet ポート自体には機能せず、Ethernet ポートの状態は VLAN インタフェースの状態の変化に応じて変化しません。

例

#VLAN インタフェース 2 をシャットダウンしてから再度開きます。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

3.1.8 vlan

Syntax

vlan { *vlan-id-list* | **all** }

undo vlan { *vlan-id-list* | **all** }

デフォルト

システムのデフォルト VLAN は 1 つだけです(VLAN 1)。

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list:VLAN リスト。vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-32>で表され、vlan-id は 1~4094 の値を取り、vlan-id2 は vlan-id1 以上の値を取り、&<1-32>は前のパラメータを最大 32 回繰り返し入力できることを示します。

all:デバイスで作成できる VLAN の最大数が 4094 時未満の場合、予約済み VLAN 以外の VLAN はサポートされません。

説明

vlan vlan-id コマンドを使用して VLAN を作成し、VLAN view に移動します。指定した VLAN がすでに存在する場合は、その VLAN view に直接移動します。

予約済みの VLAN を除き、VLAN の一括作成には **vlan vlan-id-list** コマンドが使用されます。

vlan all コマンドは、VLAN 1~4094 のバッチ作成に使用されます。

VLAN を削除するには、**undo vlan** コマンドを使用します。

デフォルト VLAN (VLAN 1)と予約済み VLAN は作成および削除できません。

動的に学習された VLAN や、他のアプリケーションによってロックされて削除されない VLAN は、**undo vlan** コマンドを使用して直接削除することはできません。対応する VLAN は、関連する設定が削除されるまで削除できません。

例

#VLAN 2 を作成し、VLAN view に移動します。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2]
```

#VLAN 4~100 および VLAN 200 を一括作成します。

```
<Sysname> system-view
[Sysname] vlan 4 to 100 200
```

関連コマンド

- **display vlan**

3.2 ポートベースのVLAN設定コマンド

3.2.1 display port

Syntax

display port { **hybrid** | **trunk** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

hybrid:デバイスに現在存在する Hybrid ポートを表示します。

trunk:デバイスに現在存在する Trunk ポートを表示します。

説明

display port コマンドは、デバイスに存在する Hybrid または Trunk ポートを表示します。

例

#現在のデバイスが存在する Hybrid ポートを表示します。

<Sysname> display port hybrid

Interface	PVID	VLAN Passing
GE1/0/1	100	Tagged: 1000, 1002, 1500, 1600-1611, 2000, 2555-2558, 3000, 4000 Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100, 150-160, 200, 255, 286, 300-302

#現在のデバイスが存在する Trunk ポートを表示します。

<Sysname> display port trunk

Interface	PVID	VLAN Passing
GE1/0/2	2	1-4, 6-100, 145, 177, 189-200, 244, 289, 400, 555, 600-611, 1000, 2006-2008

表 3-4 display port コマンドの表示情報の説明

フィールド	説明
Interface	インタフェース名
PVID	このポートのデフォルトVLAN ID
VLAN Passing	ポートが実際に通過したVLANを示します(このVLANはすでに作成されており、インタフェースで許可されています。)。

フィールド	説明
Tagged	どのVLANのメッセージがポートを通過するときにVLAN Tagを送信する必要があるかを示します。
Untagged	どのVLANのメッセージがポートを通過するかを示すVLAN Tagを削除する必要があります。

3.2.2 port

Syntax

port *interface-list*

undo port *interface-list*

デフォルト

システムはすべてのポートを VLAN 1 に接続します。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interface-list:イーサネットインタフェースのリスト。表記は interface-list ={interface-type interface-number1 [to interface-type interface-number2]}&<1-10>です。interface-type interface-number はポートタイプとポート番号、interface-number2 は interface-number1 以上の値、&<1-10>は前述のパラメータが 10 回まで入力可能であることを示します。

説明

port コマンドを使用して、VLAN に 1 つまたは一連の Access ポートを追加します。

undo port コマンドは、VLAN から 1 つまたは一連の Access ポートを削除するために使用されます。

このコマンドでは、Access ポートのみを VLAN に参加させることができ、Trunk および Hybrid ポートを VLAN に参加させることはできません。また、Access ポートを VLAN 1 に追加または削除することもできません。

デバイス上のすべてのポートのデフォルトのリンクタイプは Access タイプですが、ポートタイプはユーザが自分で切り替えることができ、詳細な設定は **port link-type** コマンドを参照してください。

例

#ポート GigabitEthernet1/0/1~GigabitEthernet1/0/3 を VLAN2 に追加します。

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/3

関連コマンド

- **display vlan**

3.2.3 port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

すべての Access ポートは VLAN 1 に属します。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id:1~4094 の範囲の値で指定された VLAN 番号。

説明

port access vlan コマンドは、指定された VLAN に Access ポートを結合するために使用されます。

undo port access vlan コマンドを使用して、デフォルトの状態を復元します。

デフォルトでは、すべての Access ポートは VLAN 1 に属しているため、このコマンドを使用して Access ポートを VLAN 1 に追加することはできません。

Access ポートが属する VLAN を別の VLAN から VLAN 1 に変更するには、**undo port access vlan** コマンドを実行します。

Access ポートは、指定された VLAN に参加する前に存在している必要があります。

例

#GigabitEthernet1/0/1 ポートを VLAN 3 に追加します。

<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit

[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port access vlan 3

3.2.4 port hybrid pvid

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

Hybrid ポートのデフォルト VLAN は、リンクタイプが Access のポートが属する VLAN です。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id:インタフェースのデフォルトの VLAN ID を指定します。範囲は 1~4094 です。

説明

port hybrid pvid コマンドを使用して、Hybrid ポートのデフォルト VLAN を設定します。

undo port hybrid pvid コマンドを使用して、Hybrid ポートのデフォルト VLAN を 1 に設定します。

Hybrid ポートで undo vlan コマンドを実行してポートのデフォルト VLAN を削除しても、ポートのデフォルト VLAN 構成は変更されません。つまり、すでに存在しない VLAN をデフォルト VLAN として使用できます。

ネイティブ Hybrid ポートのデフォルト VLAN と、接続されているピアスイッチの Hybrid ポートのデフォルト VLAN を一致させることをお勧めします。

デフォルト VLAN を設定したら、port hybrid vlan コマンドを使用して、デフォルト VLAN のメッセージが通過できるようにポートを設定し、デフォルト VLAN のメッセージを転送する必要があります。

例

#ポート GigabitEthernet1/0/1 (Hybrid 型)のデフォルト VLAN を 100 に設定し、VLAN 100 が通過できるようにします。

<Sysname> system-view
[Sysname] vlan 100

```
[Sysname-vlan100] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 untagged
```

関連コマンド

- **port hybrid vlan**
- **port link-type**

3.2.5 port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

Hybrid ポートは、リンクタイプが Access の場合にのみ、そのポートが属する VLAN のメッセージを Untagged として通過させることができます。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list :VLAN リスト、Hybrid ポートで許可される VLAN の範囲。vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-32>で表され、vlan-id は 1~4094 の値を取り、vlan-id2 は vlan-id1 以上の値を取り、&<1-32>は前のパラメータを最大 32 回繰り返し入力できることを示します。この VLAN は、デバイスで作成された VLAN である必要があります。そうでない場合、コマンドは失敗します。

tagged:このポートは、指定された VLAN メッセージを転送するときに VLAN Tag を運びます。

untagged:指定された VLAN メッセージを転送すると、ポートから VLAN Tag が削除されます。

説明

port hybrid vlan コマンドは、指定された VLAN が現在の Hybrid ポートを通過できるようにするために使用します。

undo port hybrid vlan コマンドは、指定された VLAN が現在の Hybrid ポートを通過できないようにするために使用します。

Hybrid ポートは複数の VLAN を通過させます。port hybrid vlan コマンドを複数回使用する場合、Hybrid ポートで許可される VLAN は、これらの vlan-id-list の集合です。

例

#ポート GigabitEthernet1/0/1 を Hybrid ポートに設定して、VLAN 2、4、50~VLAN 100 が通過できるようにし、これらの VLAN のメッセージを送信するときに VLAN Tag を伝送します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

- **port link-type**

3.2.6 port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

すべてのポートのリンクタイプは Access です。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

access:ポートのリンクタイプを Access タイプに設定します。

hybrid:ポートのリンクタイプを Hybrid タイプに設定します。

trunk:ポートのリンクタイプを Trunk タイプに設定します。

説明

port link-type コマンドを使用して、ポートのリンクタイプを設定します。

undo port link-type コマンドを使用して、デフォルトの状態を復元します。

Trunk ポートと Hybrid ポートを直接切り替えることはできません。他のタイプのポートに設定する前に Access ポートに設定する必要があります。

例

#ポートの設定 GigabitEthernet1/0/1 は、Trunk ポートとして設定されます。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk

3.2.7 port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

Trunk ポートは VLAN 1 のメッセージだけを通過させます。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list:VLAN リスト、Trunk ポートで許可される VLAN の範囲。vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-32>で表され、vlan-id は 1~4094 の値を取り、vlan-id2 は vlan-id1 以上の値を取り、&<1-32>は前のパラメータを最大 32 回繰り返し入力できることを示します。

all:すべての VLAN がその Trunk ポートを通過できることを示します。許可されていない VLAN のユーザがそのポートを介して制限されたリソースにアクセスできないようにするには、port trunk permit vlan all コマンドを慎重に使用することをお勧めします。

説明

port trunk permit vlan コマンドは、指定された VLAN が現在の Trunk ポートを通過できるようにするために使用します。

undo port trunk permit vlan コマンドは、指定された VLAN が現在の Trunk ポートを通過できないようにするために使用します。

Trunk ポートは複数の VLAN を通過させることができます。**port trunk permit vlan** コマンドを複数回実行した場合、Trunk ポートで許可される VLAN は、これらの vlan-id-list の集合です。

Trunk ポートから送信されるメッセージは、デフォルト VLAN のものだけが VLAN Tag を持たず、他の VLAN のものは VLAN Tag を保持する。

例

#ポート GigabitEthernet1/0/1 を Trunk ポートに設定して、VLAN 2、4、50~100 が通過できるようにします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100

関連コマンド

- **port link-type**

3.2.8 port trunk pvid

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

Trunk ポートのデフォルト VLAN は VLAN 1 です。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id:インタフェースのデフォルト値 VLAN ID を 1~4094 の範囲で指定します。

説明

port trunk pvid コマンドを使用して、Trunk ポートのデフォルト VLAN を設定します。

undo port trunk pvid コマンドを使用して、デフォルトの状態を復元します。

Trunk ポートで **undo vlan** コマンドを実行してポートのデフォルト VLAN を削除しても、ポートのデフォルト VLAN 構成は変更されません。つまり、すでに存在しない VLAN がデフォルト VLAN として使用されます。

ローカルデバイスの Trunk ポートのデフォルト VLAN ID と、接続されているピアデバイスの Trunk ポートのデフォルト VLAN ID は一致している必要があります。一致していないと、メッセージが正しく転送されません。

デフォルト VLAN を設定したら、**port trunk permit vlan** コマンドを使用して、デフォルト VLAN のメッセージが通過できるようにポートを設定し、デフォルト VLAN のメッセージを転送する必要があります。

例

#ポート GigabitEthernet1/0/1 (Trunk 型)のデフォルト VLAN を VLAN 100 に設定し、VLAN 100 が通過できるようにします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk pvid vlan 100
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 100

関連コマンド

- **port link-type**
- **port trunk permit vlan**

目次

このセクションのページは **5-x-x** です。

4 章 ループ検出 4-1
4.1 ループ検出コマンド 4-1
4.1.1 display loopback-detection 4-1
4.1.2 loopback-detection action 4-2
4.1.3 loopback-detection enable 4-4
4.1.4 loopback-detection global action 4-5
4.1.5 loopback-detection global enable 4-6
4.1.6 loopback-detection interval-time 4-7

4章 ループ検出

4.1 ループ検出コマンド

4.1.1 display loopback-detection

Syntax

display loopback-detection

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

ループ検出の設定と動作を表示するには、display loopback-detection コマンドを使用します。

例

#ループ検出の設定と動作を表示します。

<Sysname> display loopback-detection

Loop detection is enabled.

Loop detection interval is 30 second(s).

Loop is detected on following interfaces:

Interface	Action mode	VLANs
GigabitEthernet1/0/3	None	10

表 4-1 display loopback-detection コマンドの表示情報の説明

フィールド	説明
Loop detection is enabled	ループ検出がオンになっています
Loop detection is disabled	ループ検出機能がオフになっています
Loop detection interval is 30 second (s)	ループ検出の間隔は30秒です。
Loop is detected on following interfaces	次のポートでループが検出されました
Interface	ポート名

フィールド	説明
Action mode	ループ検出の処理モード: • Block:システムがポートのループを検出すると、ログ情報が生成されるだけでなく、ポートが MAC アドレスを学習してポートをブロックすることも禁止されます。 • None:システムがポートのループを検出したときに、ログ情報を生成する以外にポートを処理しない • No-learning:システムがポートのループを検出すると、ログ情報が生成されるだけでなく、ポートが MAC アドレスを学習できなくなります。 • Shutdown:システムがポートのループを検出すると、ログメッセージの生成に加えて、ポートが自動的にシャットダウンされ、メッセージを送受信できなくなります。ポートがシャットダウンされた後、自動的にリカバリできます。リカバリ時間は shutdown-interval コマンドによって決定されます。shutdown-interval コマンドの詳細は、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“3 システム管理”の”3 章 ハードウェアリソース管理”を参照してください。
VLANs	ループを生成するインタフェースで検出されたVLAN
No loop is detected	ループが検出されませんでした

4.1.2 loopback-detection action

Syntax

Layer 2 Ethernet interface view:

loopback-detection action { **block** | **no-learning** | **shutdown** }

undo loopback-detection action

Layer 2 aggregate interface view:

loopback-detection action shutdown

undo loopback-detection action

デフォルト

システムがポートのループを検出すると、そのポートは処理されず、ログ情報のみが生成されます。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

block:Block モードであることを示します。つまり、システムがポートのループを検出すると、ログ情報の生成に加えて、ポートが MAC アドレスを学習し、ポートをブロックすることを禁止します。このモードは、レイヤ 2 集約インタフェースではサポートされていません。

no-learning:No-learning モードであることを示します。つまり、システムがポートのループを検出すると、ログ情報の生成に加えて、ポートが MAC アドレスを学習できないようにします。このモードは、レイヤ 2 集約インタフェースではサポートされていません。

shutdown:Shutdown モードであることを示します。つまり、システムがポートのループを検出すると、ログメッセージの生成に加えて、ポートがメッセージを送受信できないように自動的にシャットダウンされます。シャットダウンされたポートは、**shutdown-interval** コマンドで設定された時間が経過すると自動的に再開されます。詳細は QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*3 システム管理*”の”*3 章 ハードウェアリソース管理*”を参照してください。

説明

loopback-detection action コマンドは、ループ検出の処理モードをポートに設定します。

undo loopback-detection action コマンドを使用して、デフォルトの状態を復元します。

ループ検出の処理モードは、**loopback-detection global action** コマンドを使用して System view でグローバルに設定できます。

System view の設定はすべてのポートで有効ですが、 Interface view の設定は現在のポートでのみ有効であり、 Interface view の設定の方が優先されます。

例

#ポート GigabitEthernet1/0/1 でのループ検出の処理モードを Shutdown モードに設定します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection action shutdown
```

関連コマンド

- **display loopback-detection**
- **loopback-detection global action**

4.1.3 loopback-detection enable

Syntax

loopback-detection enable vlan { *vlan-id-list* | **all** }

undo loopback-detection enable vlan { *vlan-id-list* | **all** }

デフォルト

ポートのループ検出がオフになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list:複数の VLAN の番号を示す VLAN リスト。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は指定された VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。vlan-id2 の値は vlan-id1 の値以上です。

all:作成されたすべての VLAN を示します。

説明

loopback-detection enable コマンドを使用して、ポートでループ検出機能を有効にします。

undo loopback-detection enable は、ループ検出機能をポートでオフにするために使用されます。

loopback-detection global enable コマンドを使用すると、System view でループ検出機能をグローバルに有効にできます。

デバイスグローバルまたはポートは、デバイスが送信した VLAN のループ検出メッセージをデバイスのいずれかのポートが受信すると、そのポートのループ保護アクションをトリガーするループ検出機能をオンにします。

例

#ポート GigabitEthernet1/0/1 で VLAN 10~20 のループ検出機能を有効にします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[System-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20

関連コマンド

- **display loopback-detection**
- **loopback-detection global enable**

4.1.4 loopback-detection global action

Syntax

loopback-detection global action shutdown

undo loopback-detection global action

デフォルト

システムがポートのループを検出すると、そのポートは処理されず、ログ情報のみが生成されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

shutdown:Shutdown モードであることを示します。つまり、システムがポートのループを検出すると、ログメッセージの生成に加えて、ポートがメッセージを送受信できないように自動的にシャットダウンされます。シャットダウンされたポートは、**shutdown-interval** コマンドで設定された時間が経過すると自動的に再開されます。詳細は QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*3 システム管理*”の”*3 章 ハードウェアリソース管理*”を参照してください。

説明

ループ検出の処理モードをグローバルに設定するには、**loopback-detection global action** コマンドを使用します。

undo loopback-detection global action コマンドを使用して、デフォルトの状態を復元します。

現在のポートのループ検出処理モードは、Interface view で **loopback-detection action** コマンドを使用して設定できます。

System view の設定はすべてのポートで有効ですが、 Interface view の設定は現在のポートでのみ有効であり、 Interface view の設定の方が優先されます。

例

#グローバル設定ループ検出の処理モードは Shutdown モードです。

<Sysname> system-view

[Sysname] loopback-detection global action shutdown

関連コマンド

- **display loopback-detection**
- **loopback-detection action**

4.1.5 loopback-detection global enable

Syntax

loopback-detection global enable vlan { *vlan-id-list* | **all** }

undo loopback-detection global enable vlan { *vlan-id-list* | **all** }

デフォルト

ループ検出機能はグローバルにオンになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list :複数の VLAN の番号を示す VLAN リスト。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は指定された VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。vlan-id2 の値は vlan-id1 の値以上です。

all:作成されたすべての VLAN を示します。

説明

ループ検出機能をグローバルにオンにするには、**loopback-detection global enable** コマンドを使用します。

undo loopback-detection global enable は、ループ検出機能をグローバルにオフにします。

現在のポートのループ検出機能は、Interface view で **loopback-detection enable** コマンドを使用してオンにできます。

デバイスグローバルまたはポートは、デバイスが送信した VLAN のループ検出メッセージをデバイスのいずれかのポートが受信すると、そのポートのループ保護アクションをトリガーするループ検出機能をオンにします。

例

#VLAN 10~20 内のループ検知機能をグローバルにオンにする。

<Sysname> system-view
[Sysname] loopback-detection global enable vlan 10 to 20

関連コマンド

- **display loopback-detection**
- **loopback-detection enable**

4.1.6 loopback-detection interval-time

Syntax

loopback-detection interval-time *interval*

undo loopback-detection interval-time

デフォルト

ループ検出の間隔は 5 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:ループ検出の間隔。1~300 の範囲で秒単位で指定します。

説明

loopback-detection interval-time コマンドを使用して、ループ検出の間隔を設定します。

undo loopback-detection interval-time コマンドを使用すると 30 秒に設定します。

ループ検出機能がオンになると、システムはループ検出メッセージを一定の時間間隔で送信し始め、この間隔が長いほどシステム性能の消耗が少なく、この間隔が短いほどループ検出の感度が高くなる。このコマンドを使用すると、ループ検出メッセージの送信間隔を調整して、システムのパフォーマンスとループ検出の感度のバランスをとることができます。

🕮 **メモ**:

undo loopback-detection interval-time コマンドを実行しても、デフォルト設定には戻りません。**undo** コマンドを実行した場合は、30 秒のループ検出間隔で動作する設定となります。デフォルト値に戻す場合は、**loopback-detection interval-time 5** コマンドを実行してください。

例

#ループ検出の間隔を 10 秒に設定します。

<Sysname> system-view
[Sysname] loopback-detection interval-time 10

関連コマンド

- **display loopback-detection**

目次

このセクションのページは **5-x-x** です。

5 章 STP 5-1
5.1 STP コマンド 5-1
5.1.1 active region-configuration 5-1
5.1.2 check region-configuration 5-2
5.1.3 display stp 5-3
5.1.4 display stp abnormal-port 5-12
5.1.5 display stp bpdu-statistics 5-14
5.1.6 display stp down-port 5-17
5.1.7 display stp history 5-18
5.1.8 display stp region-configuration 5-20
5.1.9 display stp root 5-21
5.1.10 display stp tc 5-22
5.1.11 instance 5-24
5.1.12 region-name 5-25
5.1.13 reset stp 5-26
5.1.14 revision-level 5-27
5.1.15 snmp-agent trap enable stp 5-28
5.1.16 stp bpdu-protection 5-29
5.1.17 stp bridge-diameter 5-30
5.1.18 stp compliance 5-31
5.1.19 stp config-digest-snooping 5-32
5.1.20 stp cost 5-33
5.1.21 stp edged-port 5-35
5.1.22 stp enable 5-36
5.1.23 stp global config-digest-snooping 5-37
5.1.24 stp global enable 5-38
5.1.25 stp global mcheck 5-39
5.1.26 stp log enable tc 5-40
5.1.27 stp loop-protection 5-41
5.1.28 stp max-hops 5-42
5.1.29 stp mcheck 5-42
5.1.30 stp mode 5-43
5.1.31 stp no-agreement-check 5-45
5.1.32 stp pathcost-standard 5-45
5.1.33 stp point-to-point 5-46
5.1.34 stp port bpdu-protection 5-48

5.1.35 stp port priority 5-49
5.1.36 stp port-log 5-51
5.1.37 stp priority 5-52
5.1.38 stp pvst-bpdu-protection 5-53
5.1.39 stp region-configuration 5-54
5.1.40 stp role-restriction 5-55
5.1.41 stp root primary 5-55
5.1.42 stp root secondary 5-57
5.1.43 stp root-protection 5-58
5.1.44 stp tc-protection 5-59
5.1.45 stp tc-protection threshold 5-60
5.1.46 stp timer forward-delay 5-60
5.1.47 stp timer hello 5-62
5.1.48 stp timer max-age 5-63
5.1.49 stp timer-factor 5-64
5.1.50 stp transmit-limit 5-65
5.1.51 stp vlan enable 5-66
5.1.52 vlan-mapping modulo 5-67

5章 STP

5.1 STPコマンド

5.1.1 active region-configuration

Syntax

active region-configuration

View

MST region view

定義済みユーザロール

network-admin

説明

active region-configuration コマンドを使用して、MST region の構成をアクティブにします。

MST region に関連するパラメータ(特に VLAN マッピングテーブル)を設定すると、スパニングツリーが再計算され、ネットワークトポロジがフラップします。ネットワークのフラッディングを軽減するために、新しく設定した MST region パラメータはすぐには有効になりませんが、このコマンドを使用してアクティブにするか、**stp global enable** コマンドを使用してスパニングツリープロトコルをグローバルに有効にします。

このコマンドを実行する前に、**check region-configuration** コマンドを使用して MST region の事前設定が正しいかどうかを確認し、これらの設定が正しいことを確認してから実行することをお勧めします。

例

#VLAN 2 を MSTI 1 にマップし、設定をアクティブにします。

<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
[Sysname-mst-region] active region-configuration

関連コマンド

- **check region-configuration**
- **instance**
- **region-name**
- **revision-level**
- **stp global enable**

- **vlan-mapping modulo**

5.1.2 check region-configuration

Syntax

check region-configuration

View

MST region view

定義済みユーザロール

network-admin

説明

check region-configuration コマンドを使用して、MST region の構成済み情報を表示します。

スパニングツリープロトコルが有効になっている 2 台以上のデバイスが同じ MST region に属するには、次の両方の条件を満たす必要があります。

- 選択係数(値は 0 で、マッチしません)、ドメイン名、リビジョンレベル、および VLAN マッピングテーブルの設定はすべて同じです。
- これらのデバイス間のリンクは共通です。

MST region の構成をアクティブ化する前に、このコマンドを使用して、MST region の事前構成が正しいことを確認し、MST region の構成をアクティブ化することをお勧めします。

例

#MST region の構成済み情報を表示します。

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
Admin Configuration
    Format selector         : 0
    Region name             : 001122334400
    Revision level          : 0
    Configuration digest : 0x3ab68794d602fdf43b21c0b37ac3bca8

    Instance   VLANs Mapped
    0          1, 3 to 4094
    15         2
```

表 5-1 check region-configuration コマンドの表示情報の説明

フィールド	説明
Format selector	スパニングツリープロトコルで指定された選択係数は0の値をとり、マッチしない.
Region name	MST region のドメイン名
Revision level	MST region のリビジョンレベル
Configuration digest	構成の概要
InstanceVLANs Mapped	MST region のVLANとMSTI間のマッピング関係、つまりVLANマッピングテーブル

関連コマンド

- **active region-configuration**
- **instance**
- **region-name**
- **revision-level**
- **vlan-mapping modulo**

5.1.3 display stp

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] [**interface** *interface-list*] [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*:指定した MSTI のスパニングツリーのステータスと統計情報を表示します。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。instance-id2 の値は instance-id1 の値以上です。ここで、 instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

vlan *vlan-id-list*:指定した VLAN のスパニングツリーステータスと統計情報を表示します。vlan-id-list は複数の VLAN を表す VLAN リストで、vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>のように表示されます。vlan-id2 の値は vlan-id1 の値以上です。ここ

で、vlan-id は VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

interface *interface-list*:指定したポートのスパニングツリーのステータスと統計情報を表示します。interface-list はポートのリストで、複数のポートを示し、interface-list ={interface-type interface-number1 [to interface-type interface-number2]}&<1-10>で表されます。interface-type interface-number2 の値は interface-type interface-number1 の値以上です。ここで、interface-type はポートタイプ、interface-number はポート番号です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

brief:スパニングツリーのステータスと統計情報の概要を表示します。このパラメータを指定しない場合、スパニングツリーのステータスと統計の詳細が表示されます。

説明

display stp コマンドを使用して、スパニングツリーのステータスと統計情報を表示します。

STP/RSTP モードの場合:

- ポートが指定されていない場合は、すべてのポートのスパニングツリーのステータスと統計情報がポート名の順に表示されます。
- ポートが指定されている場合は、そのポートのスパニングツリーのステータスと統計情報がポート名の順に表示されます。

PVST モード:

- VLAN とポートが指定されていない場合は、すべてのポート上のすべての VLAN のスパニングツリーステータスと統計情報が表示され、VLAN 番号順に表示され、各 VLAN 内でポート名順に表示されます。
- VLAN が指定されているが、ポートが指定されていない場合は、指定された VLAN のすべてのポートのスパニングツリーステータスと統計情報が表示されます。表示される情報は、VLAN 番号順に並べられ、各 VLAN 内でポート名順に並べられます。
- ポートが指定されているが、VLAN が指定されていない場合は、指定されたポート上のすべての VLAN のスパニングツリーステータスと統計情報が表示されます。表示される情報は VLAN 番号順に並べられ、各 VLAN 内でポート名順に並べられます。
- VLAN とポートの両方が指定されている場合は、指定されたポート上の指定された VLAN のスパニングツリーステータスと統計情報が表示され、VLAN 番号順に表示され、各 VLAN 内でポート名順に表示されます。

MSTP モードの場合:

- MSTI とポートが指定されていない場合は、すべてのポート上のすべての MSTI のスパニングツリーステータスと統計情報が表示されます。表示は MSTI 番号順になり、各 MSTI 内部はポート名順になります。
- MSTI が指定されているが、ポートが指定されていない場合は、指定された MSTI のすべてのポートのスパニングツリーのステータスと統計情報が表示されます。表示される情報は MSTI 番号順に並べられ、各 MSTI 内でポート名順に並べられます。
- ポートが指定されているが、MSTI が指定されていない場合は、指定されたポート上のすべての MSTI のスパニングツリーのステータスと統計情報が表示されます。表

示される情報は MSTI 番号順に並べられ、各 MSTI の内部はポート名順に並べられます。

- MSTI とポートの両方が指定されている場合は、指定されたポート上の指定された MSTI のスパニングツリーのステータスと統計情報が表示され、MSTI 番号順に表示され、各 MSTI 内部はポート名順に表示されます。

例

#MSTP モードでは、MSTI 0 のスパニングツリーステータスとポート GigabitEthernet1/0/1 の統計情報の概要が表示されます。

```
<Sysname> display stp instance 0 interface gigabitethernet 1/0/1 brief
 MST ID       Port                        Role  STP State      Protection
 0            GigabitEthernet1/0/1        ALTE  DISCARDING     LOOP
```

#PVST モードでは、ポート GigabitEthernet1/0/1 の VLAN 2 スパニングツリーのステータスと統計情報の簡単な情報が表示されます。

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp vlan 2 interface gigabitethernet 1/0/1 brief
 VLAN ID      Port                        Role  STP State      Protection
 2            GigabitEthernet1/0/1        ALTE  DISCARDING     LOOP
```

表 5-2 display stp brief コマンドの表示情報の説明

フィールド	説明
MST ID	MSTI番号
VLAN ID	VLANの番号
Port	対応するMSTIに対応するポート名
Role	ポートの役割: • ALTE:代替ポートを示します。 • BACK:バックアップポートを示します。 • ROOT:ルートポートを表します。 • DESI:指定されたポートを表します。 • MAST MAST:マスターポートを表します。 • DISA:無効ポートを示します。
STP State	ポートの状態: • FORWARDING:BPDU が送受信され、ユーザトラフィックが転送されることを示します。 • DISCARDING:BPDU は送受信できますが、ユーザトラフィックは転送されません。 • LEARNING:BPDU は送受信できるが、ユーザトラフィックは転送されない遷移状態

フィールド	説明
Protection	保護メカニズムがトリガーされると、ポートで有効になる保護のタイプ: • ROOT:ルート保護を表します。 • LOOP:ループ保護を示します。 • BPDU:BPDU 保護を示します。 • NONE:保護されていない、または構成されたスパニングツリー保護機能がトリガーされていないことを示します

#MSTP モードでは、すべてのポートのすべての MSTI のスパニングツリーステータスと統計情報の詳細が表示されます。

<Sysname> display stp

-------[CIST Global Info][Mode MSTP]-------

Bridge ID : 32768.0001-0000-0000

Bridge times : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20

Root ID/ERPC : 32768.0001-0000-0000, 0

RegRoot ID/IRPC : 32768.0001-0000-0000, 0

RootPort ID : 0.0

BPDU-Protection : Disabled

Bridge Config-

Digest-Snooping : Disabled

TC or TCN received : 2

Time since last TC : 0 days 0h:0m:58s

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----

Port protocol : Enabled

Port role : Designated Port (Boundary)

Port ID : 128.3

Port cost(Legacy) : Config=auto, Active=200

Desg.bridge/port : 32768.0001-0000-0000, 128.3

Port edged : Config=disabled, Active=disabled

Point-to-Point : Config=auto, Active=true

Transmit limit : 10 packets/hello-time

TC-Restriction : Disabled

Role-Restriction : Disabled

Protection type : Config=none, Active=none

MST BPDU format : Config=auto, Active=802.1s

Port Config-

Digest-Snooping : Disabled

Rapid transition : True

Num of VLANs mapped : 0

Port times : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 0s RemHops 20
BPDU sent : 32
TCN: 0, Config: 0, RST: 0, MST: 32
BPDU received : 2
TCN: 0, Config: 0, RST: 0, MST: 2

-------[MSTI 1 Global Info]-------
Bridge ID : 32768.0001-0000-0000
RegRoot ID/IRPC : 32768.0001-0000-0000, 0
RootPort ID : 0.0
Master bridge : 32768.0001-0000-0000
Cost to master : 0
TC received : 0

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
Port protocol : Enabled
Port role : Designated Port (Boundary)
Port ID : 128.3
Port cost(Legacy) : Config=auto, Active=200
Desg.bridge/port : 32768.0001-0000-0000, 128.3
Protection type : Config=none, Active=none
Rapid transition : True
Num of VLANs mapped : 64
Port times : RemHops 20

#PVST モードでは、すべてのポートのすべての VLAN のスパニングツリーステータスと統計情報が表示されます。

<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp
-------[VLAN 1 Global Info]-------
Protocol status : Enabled
Bridge ID : 32768.000f-e200-2200
Bridge times : Hello 2s MaxAge 20s FwdDelay 15s
VlanRoot ID/RPC : 0.00e0-fc0e-6554, 200200
RootPort ID : 128.48
BPDU-Protection : Disabled
TC or TCN received : 2
Time since last TC : 0 days 0h:5m:42s

----[Port1(GigabitEthernet1/0/1)][FORWARDING]----
Port protocol : Enabled
Port role : Designated Port
Port ID : 128.153

Port cost(Legacy) : Config=auto, Active=200
Desg. bridge/port : 32768.000f-e200-2200, 128.2
Port edged : Config=disabled, Active=disabled
Point-to-Point : Config=auto, Active=true
Transmit limit : 10 packets/hello-time
Protection type : Config=none, Active=none
Rapid transition : False
Port times : Hello 2s MaxAge 20s FwdDelay 15s MsgAge 2s

-------[VLAN 2 Global Info]-------
Protocol status : Enabled
Bridge ID : 32768.000f-e200-2200
Bridge times : Hello 2s MaxAge 20s FwDly 15s
VlanRoot ID/RPC : 0.00e0-fc0e-6554, 200200
RootPort ID : 128.48
BPDU-Protection : Disabled
TC or TCN received : 2
Time since last TC : 0 days 0h:5m:42s

#スパニングツリープロトコルが起動していない場合、スパニングツリーのステータスと統計情報が MSTP モードで表示されます。

<Sysname> display stp
Protocol status : Disabled
Protocol Std. : IEEE 802.1s
Version : 3
Bridge-Prio. : 32768
MAC address : 000f-e200-8048
Max age(s) : 20
Forward delay(s) : 15
Hello time(s) : 2
Max hops : 20
TC Snooping : Disabled

#スパニングツリープロトコルが有効になっていない場合、スパニングツリーのステータスと統計情報が PVST モードで表示されます。

<Sysname> display stp
Protocol status : Disabled
Protocol Std. : IEEE 802.1w (pvst)
Version : 2
Bridge-Prio. : 32768
MAC address : 3822-d69f-0800
Max age(s) : 20
Forward delay(s) : 15
Hello time(s) : 2

TC Snooping : Disabled

表 5-3 display stp コマンドの表示情報の説明

フィールド	説明
[CIST Global Info] [Mode MSTP]	[パブリックスパニングツリーと内部スパニングツリーのグローバル情報] [スパニングツリーの動作モード] スパニングツリーの動作モードの値は次のとおりです。 • STP • RSTP • MSTP
Bridge ID	ブリッジIDは、2つの部分で構成されます。 「.」 の前と後は、それぞれ自デバイスの優先順位と自デバイスのMACアドレスとして表されます。たとえば、「32768.000 f-e200-2200」は、デバイスの優先順位が32768で、そのMACアドレスが000 F-E200-2200であることを示します。
Bridge times	ブリッジ関連の主なパラメータ値: • Hello:Hello time タイマ値を表します。 • MaxAge:Max Age タイマ値を表します。 • FwdDelay:Forward delay タイマ値を表します。 • MaxHops:MST region の最大ホップ数
Root ID/ERPC	合計ルートID/外部パスのオーバーヘッド(つまり、このデバイスからルート全体へのパスのオーバーヘッドです。)
RegRoot ID/IRPC	ドメインルートID/内部パスのオーバーヘッド(つまり、このデバイスからドメインルートへのパスのオーバーヘッドです。)
VlanRoot ID/RPC	VLANルートブリッジID/ルートパスのオーバーヘッド(このデバイスからこのVLANルートブリッジへのパスのオーバーヘッド)
RootPort ID	ルートポートのポートID。「0.0」は、このデバイスがルートデバイスであり、ルートポートがないことを示します。
BPDU-Protection	BPDU保護機能のグローバル・オン状態
Bridge Config-Digest-Snooping	ダイジェストリスニング機能がグローバルに有効になっている状態
TC or TCN received	MSTIまたはVLANによって受信されたTCおよびTCNメッセージの数
Time since last TC	MSTIまたはVLANの最後のトポロジ変更からの経過時間

フィールド	説明
[Port1 (GigabitEthernet1/0/1)] [FORWARDING]	[インタフェースインデックス(インタフェース名)] [ポートステータス] ポートステータスの値は次のとおりです。 • Forwarding • Discarding • Learning • Disabled • ダウン
Port protocol	ポートでのスパニングツリープロトコルのオン状態
Port role	MSTIに対応するポートの役割。役割は、Alternate、Backup、Root、Designated、Master、Disabledです。
(Boundary)	これは、ポートがドメイン境界ポートであることを示します。
Port ID	ポートID
Port cost (Legacy)	ポートのパスのオーバーヘッド(Legacyは現在のデバイスのパスオーバーヘッドの計算方法を表し、dot1d-1998とdot1tの2つの計算方法があります。): • Config:構成値を表します。 • Active:実績を表します。
Desg.bridge/port	ポートの指定されたブリッジIDとポートID (ポートプライオリティをサポートしていないポートでは、ポートIDは意味を持ちません。)
Port edged	ポートがエッジポートかどうか: • Config:構成値を表します。 • Active:実績を表します。
Point-to-Point	ポートがポイントツーポイントリンクに接続されているかどうか。 • Config:構成値を表します。 • Active:実績を表します。
Transmit limit	ポートがHello Time間隔ごとに送信するメッセージの上限

フィールド	説明
Protection type	ポートは保護されていますか? • Config:構成値を表します。 • Active:保護メカニズムがトリガーされたときに有効になる保護のタイプを示す実際の値 ポートの保護タイプ: • ROOT:ルート保護を表します。 • LOOP:ループ保護を示します。 • BPDU:BPDU 保護を示します。 • PVST BPDU:MSTP の PVST BPDU 保護を示します。 • NONE:保護されていない、または構成されたスパニングツリー保護機能がトリガーされていないことを示します
TC-Restriction	ポートが開いているかどうかTC-BPDU伝播制限
Role-Restriction	ポートの役割制限が有効になっているかどうか
MST BPDU format	ポートは、legacyおよび802.1 sの値でMSTPメッセージを送信します。 • Config:構成値を表します。 • Active:実績を表します。
Port Config-Digest-Snooping	ダイジェストスヌーピング機能がポートでオンになっている
Rapid transition	ポートが現在のMSTIまたはVLANでフォワーディングステートに移行するかどうか
Num of VLANs mapped	現在のMSTI内のポートのVLAN数
Port times	ポート関連の主なパラメータ値: • Hello:Hello time タイマ値を表します。 • MaxAge:Max Age タイマ値を表します。 • FwdDelay:Forward delay タイマ値を表します。 • MsgAge:Message Age タイマ値を表します。 • RemHops:残りのホップカウント
BPDU sent	ポート送信メッセージ数
BPDU received	ポート受信メッセージ数
[MSTI 1 Global Info]	MSTIのスパニングツリーグローバル情報の指定
RegRoot ID/IRPC	MSTIドメインルート/内部パスのオーバーヘッド
Root Type	MSTIドメインルートタイプ: • Primary root:ルートブリッジを表します。 • Secondary root:バックアップルートブリッジを示します。
Master bridge	MSTIのMasterブリッジID
Cost to master	MSTIからMasterブリッジへのパスのオーバーヘッド

フィールド	説明
TC received	MSTIが受信したTCメッセージの数
[VLAN 1 Global Info]	指定されたVLANのスパニングツリーグローバル情報
Protocol status	スパニングツリープロトコルのグローバルな有効状態
Protocol Std.	スパニングツリープロトコルで使用されるプロトコル標準
Version	スパニングツリープロトコルで使用されるプロトコルのバージョン
Bridge-Prio.	MSTPモードでは、CIST内のデバイスのブリッジ優先順位を表します。PVSTモードでは、このデバイスのVLAN 1でのブリッジプライオリティを表します。
MAC address	本装置のMACアドレス
Max age (s)	BPDUの最大有効期限(PVSTモードの場合は秒、VLAN 1での設定)
Forward delay (s)	ポート状態移行の遅延(PVSTモードの場合は秒、VLAN 1での設定)
Hello time (s)	ルートデバイスがBPDUを送信する期間(PVSTモードの場合は秒、VLAN 1での設定)
Max hops	MST region の最大ホップ数
TC Snooping	TC Snoopingオン状態: • Enabled • Disabled

関連コマンド

- **reset stp**

5.1.4 display stp abnormal-port

Syntax

display stp abnormal-port

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp abnormal-port コマンドは、スパニングツリー保護機能によってブロックされたポートの履歴情報を表示するために使用されます。

スパニングツリーインスタンスまたは VLAN ごとに、最大 3 つのブロッキングポート履歴情報が表示されます。

例

#MSTP モードでは、スパニングツリー保護機能によってブロックされたポートの履歴情報が表示されます。

```
<Sysname> display stp abnormal-port
---[GigabitEthernet1/0/1]---
  MST ID    BlockReason                Time
  0         Root-Protected             14:39:04 04/15/2019
  0         Root-Protected             14:39:02 04/15/2019
  0         Root-Protected             14:39:00 04/15/2019
```

#PVST モードでは、スパニングツリー保護機能によってブロックされたポートの履歴情報が表示されます。

```
<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp abnormal-port
---[GigabitEthernet1/0/1]---
  VLAN ID   BlockReason                Time
  1         Root-Protected             14:49:17 04/15/2019
  1         Root-Protected             14:49:15 04/15/2019
  1         Root-Protected             14:49:12 04/15/2019
```

表 5-4 display stp abnormal-port コマンドの表示情報の説明

フィールド	説明
MST ID	スパニングツリー保護機能でブロックされているポートのMSTI番号
VLAN ID	スパニングツリー保護機能でブロックされているポートが存在するVLANの番号
BlockReason	ポートがブロックされる原因: • Root-Protected:ルート保護が発生したことを示します。 • Loop-Protected:ループガードが発生したことを示す • Loopback-Protected:自己ループ保護が発生したこと、すなわち、ポートが自分からプロトコルメッセージを受信したことを示す. • Disputed:指定されたポートから低プライオリティメッセージを受信し、送信ポートが Forwarding または Learning の状態であることを示す Dispute 保護が発生しました。 • InconsistentPortType-Protected:ポートタイプの一貫性のない保護が発生したことを示します。 • InconsistentPvid-Protected:PVID の矛盾した保護が発生したことを示します。

フィールド	説明
Time	保護がトリガーされた時刻

5.1.5 display stp bpdu-statistics

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-list*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したポートの BPDU 統計情報を表示します。interface-type interface-number はポートタイプとポート番号です。

instance *instance-list*:ポートで指定された MSTI の BPDU 統計情報を表示します。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。ここで、 instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。instance-id2 の値は instance-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

説明

display stp bpdu-statistics コマンドを使用して、ポートの BPDU 統計情報を表示します。

MSTP モードの場合:

- ポートと MSTI が指定されていない場合は、すべてのポートのすべての MSTI の BPDU 統計情報がポート名の順に表示され、各ポートの内部が MSTI 番号の順に表示されます。
- ポートが指定されているが、MSTI が指定されていない場合は、そのポート上のすべての MSTI の BPDU 統計情報が MSTI 番号順に表示されます。
- MSTI とポートの両方が指定されている場合は、指定されたポート上の指定された MSTI の BPDU 統計情報が表示されます。

STP/RSTP/PVST モードの場合:

- ポートが指定されていない場合は、すべてのポートの BPDU 統計情報がポート名の順に表示されます。
- ポートが指定されている場合は、そのポートの BPDU 統計情報が表示されます。

例

#MSTP モードでは、ポート GigabitEthernet1/0/1 のすべての MSTI の BPDU 統計情報が表示されます。

<Sysname> display stp bpdu-statistics interface gigabitethernet 1/0/1

Port: GigabitEthernet1/0/1

Instance-Independent:

Type	Count	Last Updated
Invalid BPDUs	0	
Looped-back BPDUs	0	
Max-aged BPDUs	0	
TCN sent	0	
TCN received	0	
TCA sent	0	
TCA received	2	10:33:12 01/13/2019
Config sent	0	
Config received	0	
RST sent	0	
RST received	0	
MST sent	4	10:33:11 01/13/2019
MST received	151	10:37:43 01/13/2019

Instance 0:

Type	Count	Last Updated
Timeout BPDUs	0	
Max-hoped BPDUs	0	
TC detected	1	10:32:40 01/13/2019
TC sent	3	10:33:11 01/13/2019
TC received	0	

#PVST モードでは、ポート GigabitEthernet1/0/1 の BPDU 統計情報が表示されます。

<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] display stp bpdu-statistics interface gigabitethernet 1/0/1

Port: GigabitEthernet1/0/1

Type	Count	Last Updated
Invalid BPDUs	0	
Looped-back BPDUs	0	

```
Max-aged BPDUs                0
TCN sent                      0
TCN received                  0
TCA sent                      0
TCA received                  2           10:33:12 01/13/2019
Config sent                   0
Config received               0
RST sent                      0
RST received                  0
MST sent                      4           10:33:11 01/13/2019
MST received                  151         10:37:43 01/13/2019
Timeout BPDUs                 0
Max-hoped BPDUs               0
TC detected                   511         10:32:40 01/13/2019
TC sent                       8844        10:33:11 01/13/2019
TC received                   1426        10:33:32 01/13/2019
PVID inconsistency BPDUs      0
```

表 5-5 display stp bpdu-statistics コマンドの表示情報の説明

フィールド	説明
Port	ポート名
Instance-Independent	MSTIIに依存しない統計
Type	統計タイプ
Count	統計値
Last Updated	最終更新時刻
Invalid BPDUs	無効なBPDUの数
Looped-back BPDUs	自己ループ(受信すると、このポートから送信されます。)のBPDUの数
Max-aged BPDUs	最大有効期限を超えるBPDUの数
TCN sent	送信されたTCNメッセージの数
TCN received	受信したTCNメッセージの数
TCA sent	発行されたTCAメッセージの数
TCA received	受信したTCAメッセージの数
Config sent	発行されたConfigurationメッセージの数
Config received	受信したConfigurationメッセージの数
RST sent	発行されたRSTP BPDUの数
RST received	受信したRSTP BPDUの数
MST sent	発行されたMSTP BPDUの数
MST received	受信したMSTP BPDUの数
Instance	指定されたMSTIIに関連する統計
Timeout BPDUs	老朽化したBPDUの数
Max-hoped BPDUs	最大ホップ数を超えるBPDUの数
TC detected	検出されたトポロジ変化の回数

フィールド	説明
TC sent	発行されたTCメッセージの数
TC received	受信したTCメッセージの数
PVID inconsistency BPDUs	受信したPVIDの不一致PVSTメッセージの数

5.1.6 display stp down-port

Syntax

display stp down-port

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp down-port コマンドは、スパニングツリー保護機能によってダウンされたポート情報を表示するために使用されます。

例

#スパニングツリー保護機能によってダウンされたポート情報を表示します。

<Sysname> display stp down-port

Down Port	Reason
GigabitEthernet1/0/1	BPDU protection

表 5-6 display stp down-port コマンドの表示情報の説明

フィールド	説明
Down Port	スパニングツリー保護機能によってドロップされたポート名
Reason	ポートダウンの原因: • BPDU protection:BPDU 保護を示す • PVST BPDU protection:MSTP の PVST BPDU 保護を示します。

5.1.7 display stp history

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **history**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*:指定された MSTI のポートロール計算の履歴情報を表示します。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。ここで、 instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。instance-id2 の値は instance-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

vlan *vlan-id-list*:指定された VLAN のポートロール計算の履歴情報を表示します。vlan-id-list は複数の VLAN を表す VLAN のリストで、vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>のように表示されます。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

説明

display stp history コマンドを使用して、スパニングツリーポートロールの計算に関する履歴情報を表示します。

STP/RSTP モードでは、表示情報はポートロールの計算された時間の早い順に並べられます。

PVST モード:

- VLAN が指定されていない場合は、すべての VLAN のポートロール計算の履歴情報が表示され、VLAN 番号順に表示され、各 VLAN 内でポートロール計算の古い順に表示されます。
- VLAN が指定されている場合は、指定された VLAN 内のポートロール計算の履歴情報が表示され、VLAN 番号順に表示され、各 VLAN 内でポートロール計算の古い順に表示されます。

MSTP モードの場合:

- MSTI が指定されていない場合は、すべての MSTI でのポートロール計算の履歴情報が表示され、MSTI 番号順に表示され、各 MSTI 内でポートロール計算の古い順に表示されます。

- MSTI が指定されている場合は、指定された MSTI におけるポートロール計算の履歴情報が表示され、 MSTI 番号順に表示情報が並び、各 MSTI 内部はポートロール計算の時系列順に並ぶ。

例

#MSTP モードでは、MSTI 2 のポートロール計算の履歴情報が表示されます。

<Sysname> display stp instance 2 history

```
---------- Instance 2 ----------

Port GigabitEthernet1/0/1
  Role change          : ROOT->DESI (Aged)
  Time                 : 2019/02/08 00:22:56
  Port priority        : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
  Designated priority  : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1

Port GigabitEthernet1/0/2
  Role change          : ALTER->ROOT
  Time                 : 2019/02/08 00:22:56
  Port priority        : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                         128.153
  Designated priority  : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
                         128.153
```

#PVST モードでは、VLAN 2 のポートロール計算の履歴情報が表示されます。

<Sysname> display stp vlan 2 history

```
---------- VLAN 2 ----------

Port GigabitEthernet1/0/1
  Role change          : ROOT->DESI (Aged)
  Time                 : 2019/02/08 00:22:56
  Port priority        : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
  Designated priority  : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1
Port GigabitEthernet1/0/2
  Role change          : ALTER->ROOT
  Time                 : 2019/02/08 00:22:56
  Port priority        : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
  Designated priority  : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

表 5-7 display stp history コマンドの表示情報の説明

フィールド	説明
Port	ポート名
Role change	ポートの役割の変更の表示(Agedはメッセージのタイムアウトによるロールの変化を表す.)

フィールド	説明
Time	ポートロールの計算時間
Port priority	ポートプライオリティ
Designated priority	優先順位の指定

5.1.8 display stp region-configuration

Syntax

display stp region-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp region-configuration コマンドを使用して、有効な MST region 構成情報を表示します。

例

#MSTP モードでは、現在有効な MST region 構成情報が表示されます。

<Sysname> display stp region-configuration
Oper Configuration
Format selector:0
Region name:hello
Revision level:0
Configuration digest :0 x5f762d9a46311effb7a488a3267fca9f

InstanceVLANs Mapped
021 to 4094
11 to 10
211 to 20

表 5-8 display stp region-configuration コマンドの表示情報の説明

フィールド	説明
Format selector	スパニングツリープロトコルで指定された選択係数。デフォルトは0、構成不可
Region name	MST region のドメイン名

フィールド	説明
Revision level	MST region のリビジョンレベル。コマンドrevision-levelを使用して設定します。デフォルトはレベル0です。
Configuration digest	構成の概要
VLANs Mapped	MSTIにマッピングされたVLAN

関連コマンド

- **instance**
- **region-name**
- **revision-level**
- **vlan-mapping modulo**

5.1.9 display stp root

Syntax

display stp root

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp root コマンドを使用して、すべてのスパニングツリーのルートブリッジ情報を表示します。

例

#MSTP モードでは、すべてのスパニングツリーのルートブリッジ情報が表示されます。

<Sysname> display stp root

MST IDRoot Bridge IDExtPathCost IntPathCost Root Port

00.00 e0-fc0e-65542002000GigabitEthernet1/0/1

#PVST モードでは、すべてのスパニングツリーのルートブリッジ情報が表示されます。

<Sysname> display stp root

VLAN IDRoot Bridge IDExtPathCost IntPathCost Root Port

10.00 e0-fc0e-65542002000GigabitEthernet1/0/1

表 5-9 display stp root コマンドの表示情報の説明

フィールド	説明
MST ID	MSTI番号
VLAN ID	VLANの番号
Root Bridge ID	ルートブリッジの番号
ExtPathCost	外部パスのオーバーヘッド。デバイスは、ポートのデフォルトのパスオーバーヘッドを自動的に計算します。ユーザは、stp costコマンドを使用して、ポートのパスオーバーヘッドを構成することもできます。
IntPathCost	内部パスのオーバーヘッド。デバイスはポートのデフォルトパスオーバーヘッドを自動的に計算し、ユーザはstp costコマンドを使用してポートのパスオーバーヘッドを構成できます。
Root Port	ルートポート情報: • 現在のデバイスのポートの 1 つが MSTI または VLAN のルートポートである場合は、ポート名が表示されます。 • ルートポートが現在のデバイスに存在しない場合は表示されません。

5.1.10 display stp tc

Syntax

display stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **tc**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*:指定した MSTI のすべてのポートが送受信した TC または TCN メッセージの数を表示します。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。ここで、 instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。instance-id2 の値は instance-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

vlan *vlan-id-list*:指定した VLAN 内のすべてのポートが送受信した TC または TCN メッセージの数を表示します。vlan-id-list は複数の VLAN を表す VLAN リストで、vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>のように表示されます。ここで、vlan-id は VLAN の番号

で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

説明

display stp tc コマンドは、スパニングツリーのすべてのポートで送受信された TC または TCN メッセージの数を表示します。

STP/RSTP モードでは、情報はポート名の順に表示されます。

PVST モード:

- VLAN が指定されていない場合は、すべての VLAN 内のすべてのポートが送受信した TC または TCN メッセージの数が表示され、VLAN 番号順に表示され、各 VLAN 内のポート名順に表示されます。
- VLAN が指定されている場合は、指定された VLAN 内のすべてのポートが送受信した TC または TCN メッセージの数が表示され、VLAN 番号順に表示され、各 VLAN 内ではポート名順に表示されます。

MSTP モードの場合:

- MSTI が指定されていない場合は、すべての MSTI において全ポートが送受信した TC または TCN メッセージ数が表示され、 MSTI 番号順に表示され、各 MSTI 内部ではポート名順に表示される。
- MSTI を指定すると、指定した MSTI 中の全ポートが送受信した TC または TCN メッセージ数が表示され、 MSTI 番号順に表示メッセージが並び、各 MSTI 内部はさらにポート名順に並ぶ。

例

#MSTP モードでは、MSTI 0 のすべてのポートで送受信された TC または TCN メッセージの数が表示されます。

<Sysname> display stp instance 0 tc

MST ID	Port	Receive	Send
0	GigabitEthernet1/0/1	6	4
0	GigabitEthernet1/0/2	0	2

#PVST モードでは、VLAN 2 のすべてのポートで送受信された TC または TCN メッセージの数が表示されます。

<Sysname> display stp vlan 2 tc

VLAN ID	Port	Receive	Send
2	GigabitEthernet1/0/1	6	4
2	GigabitEthernet1/0/2	0	2

表 5-10 display stp tc コマンドの表示情報の説明

フィールド	説明
MST ID	MSTI番号
VLAN ID	VLANの番号
Port	ポート名

フィールド	説明
Receive	ポートが受信したTCまたはTCNメッセージの数
Send	ポートが発行したTCまたはTCNメッセージの数

5.1.11 instance

Syntax

instance *instance-id* **vlan** *vlan-id-list*

undo instance *instance-id* [**vlan** *vlan-id-list*]

デフォルト

すべての VLAN は CIST (つまり MSTI 0)にマッピングされます。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

instance-id:MSTI の番号を表し、 0～4094 の範囲の値をとり、 0 は CIST を表す。undo instance コマンドを実行すると、instance-id の値の範囲は 1~4094 になります。

vlan *vlan-id-list*:VLAN を指定します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

説明

instance コマンドは、指定された VLAN を指定された MSTI にマッピングするために使用されます。

undo instance コマンドは、指定された VLAN と指定された MSTI 間のマッピング関係を削除し、これらの VLAN を CIST (MSTI 0)に再マッピングするために使用されます。

 注意

グローバルダイジェストスヌーピング機能を設定した後で次の操作を実行すると、隣接デバイスとの VLAN および MSTI マッピング関係の不一致により、ループやトラフィックの中断が発生する可能性があるため、注意してください。

- VLAN と MSTI 間のマッピング関係を変更します。

- **undo stp region-configuration** コマンドを実行して、現在のドメインの構成を解除します。

---

undo instance コマンドで VLAN が指定されていない場合、指定された MSTI にマッピングされているすべての VLAN が CIST に再マッピングされます。

同じ VLAN を異なる MSTI にマッピングすることはできません。MSTI にマッピングされている VLAN を別の MSTI に再マッピングすると、以前のマッピング関係は解除されます。

VLAN マッピング関係は、最大 65 の MSTI に対してのみ設定できます。

このコマンドを設定した後、この設定をアクティブにするには **active region-configuration** コマンドを実行する必要があります。

例

#VLAN 2 を MSTI 1 にマップします。

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
```

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**

5.1.12 region-name

Syntax

region-name *name*

undo region-name

デフォルト

MST region のドメイン名は、デバイスの MAC アドレスです。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

name:MST region のドメイン名を示す 1~32 文字の文字列。

説明

region-name コマンドを使用して、MST region のドメイン名を設定します。

undo region-name コマンドを使用して、デフォルトの状態を復元します。

MST region 名は、MST region の VLAN マッピングテーブルと MSTP のリビジョンレベルを使用して、デバイスが属する MST region を識別します。

このコマンドを設定した後、この設定をアクティブにするには **active region-configuration** コマンドを実行する必要があります。

例

#MST region のドメイン名を hello に設定します。

<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name hello

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **instance**
- **revision-level**
- **vlan-mapping modulo**

5.1.13 reset stp

Syntax

reset stp [**interface** *interface-list*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-list*:指定したポートのスパニングツリー統計情報をクリアします。interface-list はポートのリストで、複数のポートを示し、interface-list ={interface-type interface-number1 [to interface-type interface-number2]}&<1-10>で表されます。ここで、interface-type はポートタイプ、interface-number はポート番号です。interface-type interface-number2 の値は interface-type interface-number1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータを指定しないと、すべてのポートのスパニングツリー統計情報がクリアされます。

説明

reset stp コマンドは、スパニングツリーの統計情報をクリアするために使用されます。

例

#ポート GigabitEthernet1/0/1 から GigabitEthernet1/0/3 のスパニングツリー統計情報をクリアします。

<Sysname> reset stp interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3

関連コマンド

- **display stp**

5.1.14 revision-level

Syntax

revision-level *level*

undo revision-level

デフォルト

MSTP のリビジョンレベルは 0 です。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

level:MSTP のリビジョンレベルを示します。範囲は 0~65535 です。

説明

revision-level コマンドを使用して、MSTP のリビジョンレベルを設定します。

undo revision-level コマンドを使用して、デフォルトの状態を復元します。

MSTP のリビジョンレベルは、MST region 名および MST region の VLAN マッピングテーブルと共に、デバイスが属する MST region を決定するために使用される。リビジョンレベルでは、ドメイン名と VLAN マッピングテーブルが同じ場合に、異なるドメインを区別できます。

このコマンドを設定した後､この設定をアクティブにするには active region-configuration コマンドを実行する必要があります。

例

#設定デバイスの MSTP リビジョンレベルは 5 です。

<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] revision-level 5

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **instance**
- **region-name**
- **vlan-mapping modulo**

5.1.15 snmp-agent trap enable stp

Syntax

snmp-agent trap enable stp [**new-root** | **tc**]

undo snmp-agent trap enable stp [**new-root** | **tc**]

デフォルト

スパニングツリーの new-root アラーム機能がオフになっています。MSTP モードでは、スパニングツリーの TC アラーム機能は MSTI 0 でオンになり、他の MSTI ではオフになります。PVST モードでは、スパニングツリーの TC アラーム機能はすべての VLAN でオフになります。

View

System view

定義済みユーザロール

network-admin

パラメータ

new-root:STP、RSTP、または MSTP モードでは、いずれかのインスタンスで非ルートブリッジからルートブリッジとしてデバイスが選択されると、Trap メッセージが送信されます。

tc:PVST モードでは、ポートが TC メッセージを検出または受信すると、Trap メッセージが送信されます。このパラメータは、PVST モードでのみ TC アラーム機能を制御します。

説明

snmp-agent trap enable stp コマンドを使用して、スパニングツリーのアラーム機能をオンにします。

undo snmp-agent trap enable stp コマンドを使用して、スパニングツリーのアラーム機能をオフにします。

パラメータが指定されていない場合は、コマンドを実行します。

- STP、RSTP、または MSTP モードでは、スパニングツリーの new-root アラーム機能がオンまたはオフになっていることを示します。
- PVST モードでは、スパニングツリーの TC アラーム機能がオンまたはオフになっていることを示します。

例

#設定デバイスが任意のインスタンスで非ルートブリッジからルートブリッジとして選択されると、Trap メッセージが送信されます。

<Sysname> system-view
[Sysname] snmp-agent trap enable stp new-root

5.1.16 stp bpdu-protection

Syntax

stp bpdu-protection

undo stp bpdu-protection

デフォルト

グローバル BPDU ガードがオフになっている。

View

System view

定義済みユーザロール

network-admin

説明

stp bpdu-protection コマンドを使用して、グローバル BPDU ガード機能をオンにします。

undo stp bpdu-protection コマンドを使用して、グローバル BPDU ガード機能をオフにします。

このコマンドを実行すると、デバイスのエッジポートが BPDU メッセージを受信した場合は、ポートがシャットダウンされ、スパニングツリープロトコルによってシャットダウンされたことがネットワーク管理者に通知されます。シャットダウンされたポートは、**shutdown-interval** コマンドで設定できる一定の間隔が経過した後に再アクティブ化されます。**shutdown-interval** コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*3 システム管理*”の”*3 章 ハードウェアリソース管理*”を参照してください。

このコマンドは、**stp edged-port** コマンドで手動で設定したエッジポートでのみ有効です。

stp bpdu-protection コマンドと **stp port bpdu-protection** コマンドの両方が設定されている場合、1 つのポートでは **stp port bpdu-protection** コマンドの設定が優先され、そのポートで **stp port bpdu-protection** コマンドが設定されていない場合にのみグローバル設定が適用されます。

例

#グローバル BPDU ガードをオンにします。

<Sysname> system-view
[Sysname] stp bpdu-protection

関連コマンド

- **shutdown-interval (デバイス管理コマンドリファレンス/ハードウェアリソース管理)**
- **stp edged-port**
- **stp port bpdu-protection**

5.1.17 stp bridge-diameter

Syntax

stp [**vlan** *vlan-id-list*] **bridge-diameter** *diameter*

undo stp [**vlan** *vlan-id-list*] **bridge-diameter**

デフォルト

スイッチネットワークのネットワーク直径は 7 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*:PVST スイッチングネットワークで指定された VLAN のネットワーク直径を設定します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、STP/RSTP/MSTP スイッチングネットワークのネットワーク直径が設定されます。

diameter:スイッチネットワークのネットワーク直径を示し、2~7 の範囲で値を指定します。

説明

stp bridge-diameter コマンドは、スイッチネットワークのネットワーク直径、つまりスイッチネットワーク内の任意の 2 つのエンドデバイス間の最大デバイス数を設定します。

undo stp bridge-diameter コマンドを使用して、デフォルトの状態を復元します。

適切な時間パラメータ Hello Time、Forward Delay、Max Age を選択すると、スパニングツリーの収束が速くなります。これらの 3 つの時間パラメータの値はネットワークの規模に依存するため、ネットワークの直径を調整することによって、スパニングツリープロトコルはこれらの 3 つの時間パラメータの値を自動的に調整できます。ネットワーク直径がデフォルト値の 7 時の場合、3 つの時間パラメータにもそれぞれデフォルト値が設定されます。

STP/RSTP/MSTP モードでは、各 MST region は 1 つのデバイスとして扱われ、ネットワーク直径の設定は CIST に対してのみ有効で(つまり、全ルートでのみ有効です。)、MSTI に対しては無効です。

PVST モードでは、ネットワーク直径の設定は、指定された VLAN のルートブリッジでのみ有効です。

例

#MSTP モードでは、スイッチネットワークのネットワーク直径を 5 に設定します。

<Sysname> system-view
[Sysname] stp bridge-diameter 5

#PVST モードでは、スイッチネットワークで VLAN 2 のネットワーク直径を 5 に設定します。

<Sysname> system-view
[Sysname] stp vlan 2 bridge-diameter 5

関連コマンド

- **stp timer forward-delay**
- **stp timer hello**
- **stp timer max-age**

5.1.18 stp compliance

Syntax

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

デフォルト

ポートは、受信した MSTP メッセージフォーマットを自動的に認識し、認識結果に基づいて送信するメッセージフォーマットを決定します。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

auto:ポートが受信した MSTP メッセージフォーマットを自動的に認識し、認識結果に基づいて送信するメッセージフォーマットを決定することを示します。

dot1s:ポートが標準形式(802.1 s プロトコルに準拠)の MSTP メッセージのみを送信することを示します。

legacy:ポートが非標準形式と互換性のある MSTP メッセージのみを送信することを示します。

説明

stp compliance コマンドは、ポートが送受信する MSTP メッセージフォーマットを設定します。

undo stp compliance コマンドを使用して、デフォルトの状態を復元します。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#標準形式の MSTP メッセージのみを送信するようにポートを設定します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp compliance dot1s
```

5.1.19 stp config-digest-snooping

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

デフォルト

ポートのダイジェストリスニング機能がオフになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp config-digest-snooping コマンドを使用して、ポートでダイジェストリスニングを有効にします。

undo stp config-digest-snooping コマンドを使用して、ポートでダイジェストリスニング機能をオフにします。

ダイジェストスヌーピング機能は、グローバルとポートの両方で有効になっている場合にのみ有効です。ダイジェストスヌーピング機能を有効にする場合は、サードパーティ製デバイスに接続されているすべてのポートで有効にしてからグローバルに有効にすることをお勧めします。これにより、すべてのポートの設定が一度に有効になり、ネットワークへの影響が軽減されます。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#ダイジェストスヌーピングをグローバルに開始する前に、ポート GigabitEthernet1/0/1 でダイジェストスヌーピングを開始します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp global config-digest-snooping

関連コマンド

- **display stp**
- **stp global config-digest-snooping**

5.1.20 stp cost

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost** *cost-value*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **cost**

デフォルト

各スパニングツリーのパスコストは、適切な基準に従って自動的に計算されます。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*:MSTP で MSTI のパスオーバーヘッドを指定するようにポートを設定します。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。ここで、 instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。instance-id2 の値は instance-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータを指定しない場合は、MSTP CIST または STP/RSTP のポートのパスオーバーヘッドを設定します。

vlan *vlan-id-list*:PVST で指定された VLAN の設定ポートのパスオーバーヘッドを示します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

cost-value:ポートのパスオーバーヘッド値を示します。値の範囲は、ポートのデフォルトパスオーバーヘッドの計算方法によって決まります。

- IEEE 802.1D-1998 標準を使用して計算する場合、範囲は 1~65535 です。
- IEEE 802.1t 標準を使用して計算する場合、範囲は 1~2 億です。
- プライベート基準で計算する場合、値の範囲は 1~20 万です。

説明

stp cost コマンドを使用して、ポートのパスコストを設定します。

undo stp cost コマンドを使用して、デフォルトの状態を復元します。

ポートのパスコストはスパニングツリー計算の重要な要素であり、ポートの役割の選択に影響を与える可能性があります。異なるスパニングツリー上の同じポートに異なるパスコスト値を設定すると、異なる VLAN のトラフィックが異なる物理リンクに転送され、VLAN ごとの負荷分散が可能になります。

ポートのパスオーバーヘッド値が変更されると、ポートの役割が再計算され、状態が移行されます。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

MSTI と VLAN が指定されていない場合は、MSTP CIST または STP/RSTP のポートのパスオーバーヘッドを設定します。

例

#MSTP モードでは、MSTI 2 のポート GigabitEthernet1/0/1 のパスオーバーヘッド値を 200 に設定します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 2 cost 200

#PVST モードでは、VLAN 2 のポート GigabitEthernet1/0/1 のパスオーバーヘッド値を 200 に設定します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp vlan 2 cost 200

関連コマンド

- **display stp**
- **stp pathcost-standard**

5.1.21 stp edged-port

Syntax

stp edged-port

undo stp edged-port

デフォルト

ポートは非エッジポートです。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp edged-port コマンドを使用して、ポートをエッジポートとして設定します。

undo stp edged-port コマンドを使用して、デフォルトの状態を復元します。

ポートがユーザ端末に直接接続されていて、他のデバイスや共有ネットワークセグメントに接続されていない場合、そのポートはエッジポートと見なされます。ネットワークトポロジが変化しても、エッジポートに一時的なループは発生しません。したがって、

ポートがエッジポートとして設定されている場合、ポートはフォワーディングステートにすばやく移行できます。ユーザの端末に直接接続されているポートの場合、転送状態にすばやく移行できるようにエッジポートとして設定します。

エッジポートは他のデバイスに接続されていないため、他のデバイスからの BPDU は受信されません。ポートが BPDU ガード機能をオンにしていないときにポートが BPDU を受信すると、そのポートがエッジポートとして設定されていても、ポートは非エッジポートとして動作します。

エッジポートとループ保護機能の両方を同じポートに設定することはできません。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#エッジポートとしてポート GigabitEthernet1/0/1 を設定します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp edged-port
```

関連コマンド

- **stp bpdu-protection**
- **stp loop-protection**
- **stp port bpdu-protection**
- **stp root-protection**

5.1.22 stp enable

Syntax

stp enable

undo stp enable

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp enable コマンドを使用して、ポートでスパニングツリープロトコルを有効にします。

undo stp enable コマンドは、ポートでスパニングツリープロトコルをシャットダウンするために使用されます。

スパニングツリープロトコルが有効になると、デバイスは、ユーザが設定したスパニングツリーの動作モードに基づいて、STP モード、RSTP モード、PVST モード、MSTP モードのいずれで動作するかを決定します。

スパニングツリープロトコルが有効になると、システムは、受信した BPDU に基づいて対応する VLAN のスパニングツリー状態を動的に維持します。スパニングツリープロトコルが停止すると、ステータスは維持されなくなります。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#ポート GigabitEthernet1/0/1 でスパニングツリープロトコルを閉じます。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
```

関連コマンド

- **stp global enable**
- **stp mode**
- **stp vlan enable**

5.1.23 stp global config-digest-snooping

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

デフォルト

ダイジェストリスニング機能がグローバルにオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

stp global config-digest-snooping コマンドは、ダイジェストリスニング機能をグローバルに有効にするために使用します。

undo stp global config-digest-snooping コマンドを使用して、ダイジェストのリスニング機能をグローバルに停止します。

ダイジェストスヌーピング機能は、グローバルとポートの両方で有効になっている場合にのみ有効です。ダイジェストスヌーピング機能を有効にする場合は、サードパーティ製デバイスに接続されているすべてのポートで有効にしてからグローバルに有効にすることをお勧めします。これにより、すべてのポートの設定が一度に有効になり、ネットワークへの影響が軽減されます。

例

#ダイジェストスヌーピングをグローバルに開始する前に、ポート GigabitEthernet1/0/1 でダイジェストスヌーピングを開始します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp config-digest-snooping
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] stp global config-digest-snooping

関連コマンド

- **display stp**
- **stp config-digest-snooping**

5.1.24 stp global enable

Syntax

stp global enable

undo stp global enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp global enable コマンドは、スパニングツリープロトコルをグローバルに開くために使用します。

undo stp global enable コマンドは、スパニングツリープロトコルをグローバルにシャットダウンするために使用されます。

スパニングツリープロトコルが有効になると、デバイスは、ユーザが設定したスパニングツリーの動作モードに基づいて、STP モード、RSTP モード、PVST モード、MSTP モードのいずれで動作するかを決定します。

スパニングツリープロトコルが有効になると、システムは、受信した BPDU に基づいて対応する VLAN のスパニングツリー状態を動的に維持します。スパニングツリープロトコルが停止すると、ステータスは維持されなくなります。

例

#スパニングツリープロトコルをグローバルに有効にします。

<Sysname> system-view
[Sysname] stp global enable

関連コマンド

- **stp enable**
- **stp mode**

5.1.25 stp global mcheck

Syntax

stp global mcheck

View

System view

定義済みユーザロール

network-admin

説明

stp global mcheck コマンドは、mCheck 操作をグローバルに実行するために使用します。

MSTP、RSTP、または PVST を実行しているデバイスで、ポートに STP プロトコルを実行しているデバイスが接続されている場合、ポートは STP メッセージを受信すると自動的に STP モードに移行します。次の条件が満たされている場合、ポートは自動的に元のモードに移行できません。

- STP プロトコルを実行しているデバイスがシャットダウンまたはドロップされたとき。

- ポートは変更を認識できません。

この場合、mCheck を実行して手動で元のモードに戻す必要があります。

デバイスは、STP モード、RSTP モード、PVST モード、MSTP モードのいずれで実行するかを、ユーザが設定したスパニングツリーの動作モードに基づいて決定します。

このコマンドは、スパニングツリーの動作モードが MSTP モード、RSTP モード、または PVST モードの場合にのみ有効です。

例

#mCheck アクションをグローバルに実行します。

<Sysname> system-view
[Sysname] stp global mcheck

関連コマンド

- **stp mcheck**
- **stp mode**

5.1.26 stp log enable tc

Syntax

stp log enable tc

undo stp log enable tc

デフォルト

PVST モードでデバイスが TC メッセージを検出または受信すると、ログメッセージは出力されません。

View

System view

定義済みユーザロール

network-admin

説明

stp log enable tc コマンドは、デバイスが PVST モードで TC メッセージを検出または受信したときにログ情報を出力するように設定します。

undo stp log enable tc コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、PVST モードでのみ有効です。

例

#設定 PVST モードでは、デバイスは TC メッセージを検出または受信し、ログ情報を出力します。

<Sysname> system-view
[Sysname] stp log enable tc

5.1.27 stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

デフォルト

ポートのループ保護機能がオフになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp loop-protection コマンドは、ポートのループ保護機能を有効にします。

undo stp loop-protection コマンドを使用して、ポートのループ保護機能をオフにします。

エッジポートとループ保護の両方、またはルート保護とループ保護の両方を同じポートに設定することはできません。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#ポート GigabitEthernet1/0/1 でループガードをオンにします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp loop-protection

関連コマンド

- **stp edged-port**
- **stp root-protection**

5.1.28 stp max-hops

Syntax

stp max-hops *hops*

undo stp max-hops

デフォルト

MST region の最大ホップ数は 20 ホップです。

View

System view

定義済みユーザロール

network-admin

パラメータ

hops:最大ホップ数を示し、1~40 の値を取ります。

説明

stp max-hops コマンドを使用して、MST region のサイズを制限する MST region の最大ホップ数を設定します。

undo stp max-hops コマンドを使用して、デフォルトの状態を復元します。

例

#MST region の最大ホップ数を 35 ホップに設定します。

<Sysname> system-view
[Sysname] stp max-hops 35

関連コマンド

- **display stp**

5.1.29 stp mcheck

Syntax

stp mcheck

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp mcheck コマンドは、ポートで mCheck オペレーションを実行するために使用されます。

MSTP、RSTP、または PVST を実行しているデバイスで、ポートに STP プロトコルを実行しているデバイスが接続されている場合、ポートは STP メッセージを受信すると自動的に STP モードに移行します。次の条件が満たされている場合、ポートは自動的に元のモードに移行できません。

- STP プロトコルを実行しているデバイスがシャットダウンまたはドロップされたとき。
- ポートは変更を認識できません。

この場合、mCheck を実行して手動で元のモードに戻す必要があります。

STP を実行しているデバイス A、スパニングツリープロトコルを有効にしていないデバイス B、および RSTP/MSTP/PVST を実行しているデバイス C が順に接続されると、デバイス B は STP メッセージを透過し、デバイス B が接続されているデバイス C のポートは STP モードに移行します。デバイス B でスパニングツリープロトコルを有効にした後、デバイス B とデバイス C の間で RSTP/MSTP/PVST プロトコルを実行するには、デバイス B でスパニングツリーの動作モードを RSTP/MSTP/PVST に設定するだけでなく、デバイス B とデバイス C が接続されているポートで mCheck を実行します。

デバイスは、STP モード、RSTP モード、PVST モード、MSTP モードのいずれで実行するかを、ユーザが設定したスパニングツリーの動作モードに基づいて決定します。

このコマンドは、スパニングツリーの動作モードが MSTP モード、RSTP モード、または PVST モードの場合にのみ有効です。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#ポート GigabitEthernet1/0/1 で mCheck を実行します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp mcheck
```

関連コマンド

- **stp global mcheck**
- **stp mode**

5.1.30 stp mode

Syntax

stp mode { **mstp** | **pvst** | **rstp** | **stp** }

undo stp mode

デフォルト

スパニングツリーの動作モードは MSTP モードです。

View

System view

定義済みユーザロール

network-admin

パラメータ

mstp:設定スパニングツリーの動作モードは MSTP モードです。

pvst:スパニングツリーの動作モードを PVST モードに設定します。

rstp:スパニングツリーの動作モードを RSTP モードに設定します。

stp:スパニングツリーの動作モードを STP モードに設定します。

説明

stp mode コマンドを使用して、スパニングツリーの動作モードを設定します。

undo stp mode コマンドを使用して、デフォルトの状態を復元します。

MSTP モードは RSTP モードと互換性があり、RSTP モードは STP モードと互換性があります。

PVST モードと他のモードの互換性は次のとおりです。

- Access ポートの場合:PVST モードは、どの VLAN でも他のモードと互換性があります。
- Trunk ポートまたは Hybrid ポートの場合:PVST モードは、VLAN 1 でのみ他のモードと互換性があります。

例

#スパニングツリーの動作モードを STP モードに設定します。

<Sysname> system-view
[Sysname] stp mode stp

関連コマンド

- **stp enable**
- **stp global enable**
- **stp global mcheck**
- **stp mcheck**
- **stp vlan enable**

5.1.31 stp no-agreement-check

Syntax

stp no-agreement-check

undo stp no-agreement-check

デフォルト

No Agreement Check 機能がオフになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp no-agreement-check コマンドは、ポートで No Agreement Check 機能を有効にするために使用します。

undo stp no-agreement-check コマンドは、ポートで No Agreement Check 機能をオフにするために使用されます。

この機能は、がルートポートでオンになっている場合にのみ有効です。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#ポート GigabitEthernet1/0/1 で No Agreement Check を有効にします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp no-agreement-check

5.1.32 stp pathcost-standard

Syntax

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

デフォルト

デフォルトのパスコストは legacy で計算されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

dot1d-1998:デフォルトのパスのオーバーヘッドが IEEE 802.1D-1998 標準で計算されることを示します。

dot1t:デフォルトのパスのオーバーヘッドが IEEE 802.1t 標準で計算されることを示します。

legacy:デフォルトのパスのオーバーヘッドがプライベート標準で計算されることを示します。

説明

stp pathcost-standard コマンドを使用して、デフォルトのパスコストの計算基準を構成します。

undo stp pathcost-standard コマンドを使用して、デフォルトの状態を復元します。

デフォルトのパスコストの計算基準を変更すると、ポートのパスコストがデフォルト値に戻ります。

例

#構成デフォルトのパスのオーバーヘッドは、IEEE 802.1D-1998 標準に従って計算されます。

<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998

関連コマンド

- **display stp**
- **stp cost**

5.1.33 stp point-to-point

Syntax

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

デフォルト

ポートのリンクタイプは auto です。つまり、このポートに接続されているリンクがポイントツーポイントリンクであるかどうかがシステムによって自動的に検出されます。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

auto:自ポートに接続されているリンクがポイントツーポイントリンクかどうかを自動的に検出することを示す。

force-false:このポートに接続されているリンクがポイントツーポイントリンクではないことを示します。

force-true:このポートに接続されているリンクがポイントツーポイントリンクであることを示します。

説明

stp point-to-point コマンドを使用して、ポートのリンクタイプを設定します。

undo stp point-to-point コマンドを使用して、デフォルトの状態を復元します。

ポートが非ポイントツーポイントリンクに接続されている場合、ポートの状態は迅速に移行できません。

ポートがレイヤ 2 集約インタフェースであるか、全二重モードで動作している場合は、ポイントツーポイントリンクに接続するようにポートを構成できます。通常は、システムが自動的に検出するデフォルトの構成を使用することをお勧めします。

MSTP モードまたは PVST モードでは、ポートにコマンド **stp point-to-point force-false** またはコマンド **stp point-to-point force-true** が設定されている場合、その設定はそのポートが属するすべての MSTI に対して有効です。

ポートがポイントツーポイントリンクに接続するように設定されていても、そのポートに実際に接続されている物理リンクがポイントツーポイントリンクでない場合は、一時的なループが発生する可能性があります。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#設定ポート GigabitEthernet1/0/1 に接続されるリンクはポイントツーポイントリンクです。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp point-to-point force-true
```

関連コマンド

- **display stp**

5.1.34 stp port bpdu-protection

Syntax

stp port bpdu-protection { **enable** | **disable** }

undo stp port bpdu-protection

デフォルト

ポートの BPDU 保護機能のオン/オフは設定されていません。デフォルトでは、グローバル BPDU ガードがオンの場合、エッジポートの BPDU ガードがオンになっています。グローバル BPDU ガードがオフの場合、エッジポートの BPDU ガードはオフになります。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

enable:ポートの BPDU ガード機能がオンになっていることを示します。

disable:ポートの BPDU ガード機能がオフになっていることを示します。

説明

stp port bpdu-protection コマンドを使用して、ポートの BPDU ガード機能を設定します。

undo stp port bpdu-protection コマンドを使用して、デフォルトの状態を復元します。

ポートで **stp port bpdu-protection enable** コマンドを設定した後、ポートが BPDU を受信すると、システムはポートをシャットダウンし、スパニングツリープロトコルによってポートがシャットダウンされたことをネットワーク管理者に通知します。シャットダウンされたポートは、**shutdown-interval** コマンドで設定できる一定の間隔が経過した後に再アクティブ化されます。**shutdown-interval** コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの*“3 システム管理”の”3 章 ハードウェアリソース管理”*を参照してください。

stp bpdu-protection コマンドと **stp port bpdu-protection** コマンドの両方が設定されている場合、1 つのポートでは **stp port bpdu-protection** コマンドの設定が優先され、そのポートで **stp port bpdu-protection** コマンドが設定されていない場合にのみグローバル設定が適用されます。

レイヤ 2 イーサネットポートビューの下の設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#ポート GigabitEthernet1/0/1 を設定して、BPDU ガード機能をオンにします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp port bpdu-protection enable

関連コマンド

- **shutdown-interval (デバイス管理コマンドリファレンス/ハードウェアリソース管理)**
- **stp bpdu-protection**
- **stp edged-port**

5.1.35 stp port priority

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **port priority**

デフォルト

ポートのプライオリティは 128 です。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*:MSTP で MSTI の優先順位を指定するようにポートを設定します。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。ここで、 instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。instance-id2 の値は instance-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、MSTP CIST または STP/RSTP でポートのプライオリティを設定します。

vlan *vlan-id-list*:PVST で VLAN のプライオリティを指定するようにポートを設定します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

priority:ポートのプライオリティを、0、16、32 などの 16 ステップで 0~240 の範囲で指定します。

説明

stp port priority コマンドを使用して、ポートのプライオリティを設定します。ポートプライオリティは、ビルドツリーでのポートの役割選択に影響を与える可能性があります。

undo stp port priority コマンドを使用して、デフォルトの状態を復元します。

通常、ポートプライオリティの値が小さいほど、ポートのプライオリティは高くなります。デバイスのすべてのポートで同じプライオリティ値が使用されている場合、ポートのプライオリティの高さはポートのインデックス番号のサイズによって決まります。つまり、インデックス番号が小さいほどプライオリティが高くなります。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

MSTI と VLAN が指定されていない場合は、MSTP CIST または STP/RSTP でポートのプライオリティが設定されています。

例

#MSTP モードでは、MSTI 2 のポート GigabitEthernet1/0/1 のプライオリティを 16 に設定します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp instance 2 port priority 16
```

#PVST モードでは、VLAN 2 のポート GigabitEthernet1/0/1 のプライオリティを 16 に設定します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp vlan 2 port priority 16
```

関連コマンド

- **display stp**

5.1.36 stp port-log

Syntax

stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

undo stp port-log { **all** | **instance** *instance-list* | **vlan** *vlan-id-list* }

デフォルト

ポート状態変化メッセージスイッチがオフになっていることを示します。

View

System view

定義済みユーザロール

network-admin

パラメータ

all:MSTP/PVST すべての MSTI/VLAN のポート状態変化情報表示スイッチをオンまたはオフにします。

instance *instance-list*:MSTP をオンまたはオフにする MSTI のポート状態変化情報表示スイッチを指定します。MSTI 0 が指定されている場合は、STP/RSTP のポート状態変化情報表示スイッチをオンまたはオフにします。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。ここで、instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。instance-id2 の値は instance-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

vlan *vlan-id-list*:PVST をオンまたはオフにすることを示します指定した VLAN のポートステータス変更メッセージ表示スイッチ。vlan-id-list は VLAN のリストで、vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>で表されます。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

説明

stp port-log コマンドは、ポートの状態変化情報表示スイッチをオンにします。

undo stp port-log コマンドは、ポートの状態変化情報表示スイッチをオフにします。

例

#MSTP モードでは、MSTI 2 のポート状態変化情報表示スイッチをオンにします。

```
<Sysname> system-view
[Sysname] stp port-log instance 2
%Aug 16 00:49:41:856 2019 Sysname STP/3/STP_DISCARDING: Instance 2's port GigabitEthernet1/0/1 has been set to discarding state.
```

%Aug 16 00:49:41:856 2019 Sysname STP/3/STP_FORWARDING: Instance 2's port GigabitEthernet1/0/2 has been set to forwarding state.

///この情報は、MSTI 2 で GigabitEthernet1/0/1 のポートステータスが Discarding になり、GigabitEthernet1/0/2 のポートステータスが Forwarding になることを示しています。

#PVST モードでは、VLAN 1~4094 のポート状態変化情報表示スイッチを ON にします。

<Sysname> system-view
[Sysname] stp port-log vlan 1 to 4094
%Aug 16 00:49:41:856 2019 Sysname STP/3/STP_DISCARDING:VLAN 2's GigabitEthernet1/0/1 has been set to discarding state.
%Aug 16 00:49:41:856 2019 Sysname STP/3/STP_FORWARDING:VLAN 2's GigabitEthernet1/0/2 has been set to forwarding state.

///この情報は、VLAN 2 で GigabitEthernet1/0/1 のポートステータスが Discarding になり、GigabitEthernet1/0/2 のポートステータスが Forwarding になることを示しています。

5.1.37 stp priority

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority** *priority*

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **priority**

デフォルト

デバイスの優先度は 32768 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*:MSTP で MSTI の優先順位を指定するようにデバイスを設定します。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。ここで、 instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。instance-id2 の値は instance-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータを指定しない場合は、MSTP CIST または STP/RSTP でデバイスの優先順位を設定します。

vlan *vlan-id-list*:PVST で VLAN のプライオリティを指定するようにデバイスを設定します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。

vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

priority:デバイスの優先度を示します。値が小さいほど優先度が高くなります。値の範囲は 0~61440 で、ステップサイズは 4096 です。つまり、デバイスは 0、4096、8192 などの 16 個の優先順位値を設定できます。

説明

stp priority コマンドを使用して、デバイスの優先順位を設定します。

undo stp priority コマンドを使用して、デフォルトの状態を復元します。

MSTI と VLAN が指定されていない場合は、MSTP CIST または STP/RSTP でデバイスの優先順位が設定されています。

例

#MSTP モードでは、MSTI 1 のデバイスの優先順位を 4096 に設定します。

<Sysname> system-view
[Sysname] stp instance 1 priority 4096

#PVST モードでは、VLAN 1 でデバイスのプライオリティを 4096 に設定します。

<Sysname> system-view
[Sysname] stp vlan 1 priority 4096

5.1.38 stp pvst-bpdu-protection

Syntax

stp pvst-bpdu-protection

undo stp pvst-bpdu-protection

デフォルト

MSTP の PVST メッセージ保護機能はオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

stp pvst-bpdu-protection コマンドを使用して、MSTP の PVST メッセージ保護機能を有効にします。

undo stp pvst-bpdu-protection コマンドを使用して、MSTP の PVST メッセージ保護機能をオフにします。

MSTP モードでは、デバイスで PVST メッセージ保護が有効になっている場合、一部のポートで PVST メッセージが受信されると、システムはポートをシャットダウンします。シャットダウンされたポートは、shutdown-interval コマンドで設定された一定の間隔が経過した後、自動的に再オープンされます。

例

#MSTP モードで、MSTP の PVST メッセージ保護機能をオンにします。

<Sysname> system-view
[Sysname] stp pvst-bpdu-protection

関連コマンド

- **shutdown-interval (デバイス管理コマンドリファレンス/ハードウェアリソース管理)**

5.1.39 stp region-configuration

Syntax

stp region-configuration

undo stp region-configuration

デフォルト

MST region の 3 つのパラメータはデフォルト値を使用します。MST region 名はデバイスのブリッジ MAC アドレスで、すべての VLAN は CIST にマップされ、MSTP リビジョンレベルは 0 です。

View

System view

定義済みユーザロール

network-admin

説明

stp region-configuration コマンドを使用して、MST region view にアクセスします。

undo stp region-configuration コマンドは、MST region の構成をデフォルト値に戻すために使用します。

MST region view に移動すると、MST region に関連するパラメータ(ドメイン名、VLAN マッピングテーブル、およびリビジョンレベル)を構成できます。

例

#MST region view に入ります。

<Sysname> system-view
[Sysname] stp region-configuration

[Sysname-mst-region]

5.1.40 stp role-restriction

Syntax

stp role-restriction

undo stp role-restriction

デフォルト

ポートロール制限機能がオフになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp role-restriction コマンドを使用して、ポートロール制限機能を有効にします。

undo stp role-restriction コマンドを使用して、ポートロール制限機能をオフにします。

ポートの役割制限機能を有効にすると、そのポートはルートポートとして計算されません。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#ポート GigabitEthernet1/0/1 のポートロール制限機能を有効にします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp role-restriction

5.1.41 stp root primary

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root primary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

デフォルト

設備はルートブリッジではありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*:現在のデバイスが MSTP の MSTI を指定するルートブリッジを設定します。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。ここで、 instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。instance-id2 の値は instance-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

vlan *vlan-id-list*:現在のデバイスが PVST に VLAN を割り当てるルートブリッジを設定していることを示します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

説明

stp root primary コマンドを使用して、デバイスをルートブリッジとして設定します。

undo stp root コマンドを使用して、デフォルトの状態を復元します。

デバイスがルートブリッジとして設定されると、デバイスの優先順位を変更できなくなります。

MSTI と VLAN が指定されていない場合は、現在のデバイスが MSTP CIST または STP/RSTP であるルートブリッジが設定されています。

例

#MSTP モードで、デバイスを MSTI 1 のルートブリッジに設定します。

```
<Sysname> system-view
[Sysname] stp instance 1 root primary
```

#PVST モードで、デバイスを VLAN 1 のルートブリッジに設定します。

```
<Sysname> system-view
[Sysname] stp vlan 1 root primary
```

関連コマンド

- **stp priority**
- **stp root secondary**

5.1.42 stp root secondary

Syntax

stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root secondary**

undo stp [**instance** *instance-list* | **vlan** *vlan-id-list*] **root**

デフォルト

デバイスはバックアップルートブリッジではありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*:現在のデバイスが MSTP の MSTI を指定するバックアップルートブリッジを設定していることを示します。instance-list は複数の MSTI を表す MSTI リストで、instance-list ={instance-id1 [to instance-id2]}&<1-10>で表されます。ここで、instance-id は MSTI の番号であり、 0～4094 の範囲の値をとり、 0 は CIST を表す。instance-id2 の値は instance-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

vlan *vlan-id-list*:現在のデバイスが PVST に VLAN を指定するバックアップルートブリッジを設定していることを示します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

説明

stp root secondary コマンドは、バックアップルートブリッジとしてデバイスを設定するために使用します。

undo stp root コマンドを使用して、デフォルトの状態を復元します。

デバイスがルートブリッジをバックアップするように設定されると、そのデバイスの優先順位を変更できなくなります。

MSTI と VLAN が指定されていない場合は、現在のデバイスが MSTP CIST または STP/RSTP であるバックアップルートブリッジが設定されています。

例

#MSTP モードで、デバイス MSTI 1 のバックアップルートブリッジを設定します。

<Sysname> system-view
[Sysname] stp instance 1 root secondary

#PVST モードで、デバイスを VLAN 1 のバックアップルートブリッジに設定します。

<Sysname> system-view
[Sysname] stp vlan 1 root secondary

関連コマンド

- **stp priority**
- **stp root primary**

5.1.43 stp root-protection

Syntax

stp root-protection

undo stp root-protection

デフォルト

ポートのルート保護がオフになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp root-protection コマンドは、ポートのルート保護を有効にします。

undo stp root-protection コマンドを使用して、ポートのルート保護機能をオフにします。

同じポートで、ルート保護機能とループ保護機能を同時に設定することはできません。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#ポート GigabitEthernet1/0/1 でルート保護を有効にします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp root-protection

関連コマンド

- **stp edged-port**
- **stp loop-protection**

5.1.44 stp tc-protection

Syntax

stp tc-protection

undo stp tc-protection

デフォルト

TC-BPDU 攻撃からの保護がオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

stp tc-protection コマンドは、TC-BPDU 攻撃からの保護を有効にするために使用します。

undo stp tc-protection コマンドは、TC-BPDU 攻撃からの保護を無効にするために使用します。

TC-BPDU 攻撃からの保護が有効になっている場合、デバイスが単位時間(10 秒に固定)に TC-BPDU を受信する回数が **stp tc-protection threshold** コマンドで指定された最大回数(N 回とします)を超えると、デバイスはこの間に N 回だけ転送アドレステーブルエントリをリフレッシュします。一方、N 回を超える TC-BPDU の場合、デバイスはこの間にもう一度アドレステーブルエントリをリフレッシュするので、転送アドレステーブルエントリの頻繁なリフレッシュを回避できます。

例

#TC-BPDU 攻撃からの保護をオフにします。

<Sysname> system-view
[Sysname] undo stp tc-protection

関連コマンド

- **stp tc-protection threshold**

5.1.45 stp tc-protection threshold

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

デフォルト

デバイスが TC-BPDU を受信した直後に転送アドレステーブルエントリを更新する最大回数は、単位時間(10 秒に固定)あたり 6 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

number:デバイスがTC-BPDUを受信した直後に転送アドレステーブルエントリを更新した、単位時間当たりの最大回数(10 秒に固定)。範囲は 1~255 です。

説明

stp tc-protection threshold コマンドを使用して、デバイスが TC-BPDU を受信してから一定の時間内に、TC-BPDU の受信直後に転送アドレステーブルエントリを更新できる単位時間(10 秒に固定)あたりの最大回数を設定します。

undo stp tc-protection threshold コマンドを使用して、デフォルトの状態を復元します。

例

#設定ユニット時間(10 秒に固定)で、デバイスが TC-BPDU を受信してから一定時間内に、TC-BPDU の受信直後に転送アドレステーブルエントリを更新できる最大回数は 10 です。

<Sysname> system-view
[Sysname] stp tc-protection threshold 10

関連コマンド

- **stp tc-protection**

5.1.46 stp timer forward-delay

Syntax

stp [**vlan** *vlan-id-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-id-list*] **timer forward-delay**

デフォルト

Forward Delay は 1500 センチ秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*:VLAN の Forward Delay 時間パラメータを指定するように PVST を設定します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、STP/RSTP/MSTP の Forward Delay 時間パラメータが設定されています。

time:400~3000 の範囲で Forward Delay を表す時間値。ステップは 100 で、単位はセンチ秒です。

説明

stp timer forward-delay コマンドは、Forward Delay 時間パラメータを設定するために使用します。

undo stp timer forward-delay コマンドを使用して、デフォルトの状態を復元します。

Forward Delay 状態移行の遅延時間を決定するために使用されます。一時的なループが発生しないようにするために、スパニングツリープロトコルでは、ポートが Discarding 状態から Forwarding 状態に移行するときの遷移として Learning 状態を設定し、リモートデバイスの状態切り替えと同期して状態の移行に Forward Delay 時間の待機が必要であることを指定しています。

通常、このコマンドを使用して Forward Delay 時間パラメータを直接調整することはお勧めしません。この時間パラメータの値はネットワークの規模に依存するため、stp bridge-diameter コマンドを使用してネットワークの直径を調整することにより、スパニングツリープロトコルでこの時間パラメータの値を自動的に調整することをお勧めします。ネットワーク直径にデフォルト値を設定すると、時間パラメータにもデフォルト値が設定されます。

例

#MSTP モードでは、Forward Delay を 2000 センチ秒に設定します。

```
<Sysname> system-view
[Sysname] stp timer forward-delay 2000
```

#PVST モードでは、VLAN 2 の Forward Delay を 2000 センチ秒に設定します。

```
<Sysname> system-view
```

[Sysname] stp vlan 2 timer forward-delay 2000

関連コマンド

- **stp bridge-diameter**
- **stp timer hello**
- **stp timer max-age**

5.1.47 stp timer hello

Syntax

stp [**vlan** *vlan-id-list*] **timer hello** *time*

undo stp [**vlan** *vlan-id-list*] **timer hello**

デフォルト

Hello Time は 200 センチ秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*:VLAN の Hello Time 時間パラメータを指定するように PVST を設定します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、STP/RSTP/MSTP の Hello Time 時間パラメータが設定されています。

time:100~1000 の範囲で Hello Time を表す時間値。ステップは 100 で、単位はセンチ秒です。

説明

stp timer hello コマンドは、Hello Time 時間パラメータを設定するために使用します。

undo stp timer hello コマンドを使用して、デフォルトの状態を復元します。

Hello Time リンクに障害があるかどうかを検出します。スパニングツリープロトコルは、リンクに障害があるかどうかを確認するために、Hello Time ごとに BPDU を送信します。デバイスが Hello Time 時間内に BPDU を受信しない場合、メッセージのタイムアウトが原因でスパニングツリーが再計算されます。

通常、このコマンドを使用して Hello Time 時間パラメータを直接調整することはお勧めしません。この時間パラメータの値はネットワークの規模に依存するため、**stp bridge-diameter** コマンドを使用してネットワークの直径を調整することにより、スパニ

ングツリープロトコルでこの時間パラメータの値を自動的に調整することをお勧めします。ネットワーク直径にデフォルト値を設定すると、時間パラメータにもデフォルト値が設定されます。

例

#MSTP モードでは、Hello Time を 400 センチ秒に設定します。

<Sysname> system-view
[Sysname] stp timer hello 400

#PVST モードでは、VLAN 2 の Hello Time を 400 センチ秒に設定します。

<Sysname> system-view
[Sysname] stp vlan 2 timer hello 400

関連コマンド

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer max-age**

5.1.48 stp timer max-age

Syntax

stp [**vlan** *vlan-id-list*] **timer max-age** *time*

undo stp [**vlan** *vlan-id-list*] **timer max-age**

デフォルト

Max Age は 2000 センチ秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*:VLAN の Max Age 時間パラメータを指定するように PVST を設定します。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、STP/RSTP/MSTP の Max Age 時間パラメータが設定されています。

time:Max Age を表す時間値。600~4000 の値をとり、歩幅は 100 分の 1 センチ秒です。

説明

stp timer max-age コマンドは、Max Age 時間パラメータを設定するために使用します。

undo stp timer max-age コマンドを使用して、デフォルトの状態を復元します。

Max Age BPDU がタイムアウトしたかどうかを確認するために使用します。MSTP の CIST では、デバイスは Max Age 時間に基づいて、ポートが受信した BPDU がタイムアウトしたかどうかを判断します。ポートが受信した BPDU がタイムアウトになった場合は、MSTI を再計算する必要があります。Max Age MSTP に対する MSTI 時刻が無効です。

通常、このコマンドを使用して Max Age 時間パラメータを直接調整することはお勧めしません。この時間パラメータの値はネットワークの規模に依存するため、**stp bridge-diameter** コマンドを使用してネットワークの直径を調整することにより、スパニングツリープロトコルでこの時間パラメータの値を自動的に調整することをお勧めします。ネットワーク直径にデフォルト値を設定すると、時間パラメータにもデフォルト値が設定されます。

例

#MSTP モードでは、Max Age を 1000 センチ秒に設定します。

<Sysname> system-view
[Sysname] stp timer max-age 1000

#PVST モードでは、VLAN 2 の Max Age を 1000 センチ秒に設定します。

<Sysname> system-view
[Sysname] stp vlan 2 timer max-age 1000

関連コマンド

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer hello**

5.1.49 stp timer-factor

Syntax

stp timer-factor *factor*

undo stp timer-factor

デフォルト

タイムアウト時間係数は 3 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

factor:タイムアウト時間の係数を表し、1~20 の値を取ります。

説明

stp timer-factor コマンドを使用して、デバイスのタイムアウト時間を決定するタイムアウト時間係数を設定します。タイムアウト時間=タイムアウト時間係数×3×Hello Time です。

undo stp timer-factor コマンドを使用して、デフォルトの状態を復元します。

ネットワークトポロジが安定すると、非ルートブリッジデバイスは、ルートブリッジから送信された BPDU を Hello Time 時間ごとに周囲の接続デバイスに転送して、リンクに障害がないかどうかを確認します。通常、アップストリームデバイスからの BPDU がデバイスによって 9 倍の Hello Time 時間内に受信されない場合、アップストリームデバイスはダウンしていると見なされ、スパニングツリーの計算が再開されます。

次の場合は、デバイスのタイムアウト時間係数を 5~7 に設定することをお勧めします。

- バックエンドデバイスからの BPDU が長時間受信されないことがあります。これは、バックエンドデバイスのビジー状態が原因である可能性があります(たとえば、エンドツーエンドのデバイスに多数のレイヤ 2 インタフェースが設定されている場合)。この場合、スパニングツリーの再計算は通常行われず、バックエンドデバイスのタイムアウトを延長する必要があります。
- 安定したネットワークでは、タイムアウト時間を長くすることでネットワーク資源の無駄を減らすことができる。

例

#タイムアウト時間係数を 7 に設定します。

```
<Sysname> system-view
[Sysname] stp timer-factor 7
```

関連コマンド

- **stp timer hello**

5.1.50 stp transmit-limit

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

デフォルト

ポートが BPDU を送信するレートは 10 です。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

limit:ポートが BPDU を送信するレートを示します。範囲は 1~255 です。

説明

stp transmit-limit コマンドを使用して、ポートが BPDU を送信するレートを設定します。

undo stp transmit-limit コマンドを使用して、デフォルトの状態を復元します。

Hello Time 時間あたりにポートが送信できる BPDU の最大数=ポートが BPDU を送信するレート+Hello Time 時間。

ポートが BPDU を送信するレートが高いほど、Hello Time あたりに送信できる BPDU の数が多くなり、使用されるシステム・リソースも増えます。送信レートを適切に設定すると、一方ではポートが BPDU を送信する速度を制限できますが、他方では、ネットワークトポロジが不安定な場合にスパニングツリープロトコルが帯域幅リソースを過度に消費することを防止できます。デフォルト構成を使用することをお勧めします。

レイヤ 2 イーサネットインタフェースビューの設定は、現在のポートに対してのみ有効です。Layer 2 aggregate interface view の下の構成は、現在のインタフェースに対してのみ有効です。集約メンバー・ポートの構成は、メンバー・ポートが集約グループを終了するまで有効になりません。

例

#ポート GigabitEthernet1/0/1 が BPDU を送信するレートを 5 に設定します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] stp transmit-limit 5
```

5.1.51 stp vlan enable

Syntax

stp vlan *vlan-id-list* **enable**

undo stp vlan *vlan-id-list* **enable**

デフォルト

VLAN でスパニングツリープロトコルが有効になっている。

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*:指定した VLAN でスパニングツリープロトコルのオン/オフを切り替えます。vlan-id-list は、複数の VLAN を表す VLAN リストです。表示形式は vlan-id-list ={vlan-id1 [to vlan-id2]}&<1-10>です。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。vlan-id2 の値は vlan-id1 の値以上です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。

説明

stp vlan enable コマンドを使用して、VLAN でスパニングツリープロトコルを有効にします。

undo stp enable コマンドは、VLAN でスパニングツリープロトコルをシャットダウンするために使用されます。

スパニングツリープロトコルが有効になると、デバイスは、ユーザが設定したスパニングツリーの動作モードに基づいて、STP モード、RSTP モード、MSTP モード、PVST モードのいずれで動作するかを決定します。

スパニングツリープロトコルが有効になると、システムは、受信した BPDU に基づいて対応する VLAN のスパニングツリー状態を動的に維持します。スパニングツリープロトコルが停止すると、ステータスは維持されなくなります。

例

#PVST モードでは、スパニングツリープロトコルをグローバルに有効にしてから、VLAN 2 で有効にします。

<Sysname> system-view
[Sysname] stp mode pvst
[Sysname] stp global enable
[Sysname] stp vlan 2 enable

関連コマンド

- **stp enable**
- **stp global enable**
- **stp mode**

5.1.52 vlan-mapping modulo

Syntax

vlan-mapping modulo *modulo*

デフォルト

すべての VLAN は CIST (つまり MSTI 0)にマッピングされます。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

modulo:マグニチュードを 1~64 の範囲で表します。

説明

vlan-mapping modulo コマンドを使用すると、現在の MST region 内のすべての VLAN が、指定したモジュロ値で異なる MSTI にマッピングされるように、VLAN マッピングテーブルをすばやく設定できます。

同じ VLAN を異なる MSTI にマッピングすることはできません。MSTI にマッピングされている VLAN を別の MSTI に再マッピングすると、以前のマッピング関係は解除されます。

このコマンドは、VLAN を(VLAN ID - 1)%modulo +1 という番号の MSTI にマッピングします。ここで、(VLAN ID - 1)%modulo は(VLAN ID - 1)のマグニチュード計算を表します。マグニチュードが 15 の場合、VLAN 1 は MSTI 1 に、VLAN 2 は MSTI 2 に、.....は MSTI 15 に、VLAN 15 VLAN ID - 1 は MSTI 1 にマップされます。

例

#すべての VLAN を異なる MSTI にモデル 8 でマッピングします。

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **region-name**
- **revision-level**

目次

このセクションのページは **5-x-x** です。

6 章 LLDP 6-1
6.1 LLDP コマンド 6-1
6.1.1 display lldp local-information 6-1
6.1.2 display lldp neighbor-information 6-7
6.1.3 display lldp statistics 6-14
6.1.4 display lldp status 6-17
6.1.5 display lldp tlv-config 6-21
6.1.6 lldp admin-status 6-25
6.1.7 lldp check-change-interval 6-26
6.1.8 ldp enable 6-27
6.1.9 lldp encapsulation snap 6-28
6.1.10 lldp fast-count 6-29
6.1.11 lldp global enable 6-29
6.1.12 lldp hold-multiplier 6-30
6.1.13 lldp management-address-format string 6-31
6.1.14 lldp notification med-topology-change enable 6-32
6.1.15 lldp timer notification-interval 6-33
6.1.16 lldp timer reinit-delay 6-34
6.1.17 lldp timer tx-interval 6-35
6.1.18 lldp tlv-enable 6-35
6.1.19 reset lldp statistics 6-41

6章 LLDP

6.1 LLDPコマンド

6.1.1 display lldp local-information

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global:グローバル LLDP ローカル情報を表示します。

interface *interface-type interface-number*:指定したインタフェースの LLDP ローカル情報を表示します。interface-type interface-number はインタフェースタイプとインタフェース番号を示します。

説明

display lldp local-information コマンドを使用して、LLDP ローカル情報を表示します。

パラメータが指定されていない場合は、グローバル LLDP 情報と、LLDP 機能がオンで up 状態のすべてのインタフェースの LLDP 情報を含む、すべての LLDP ローカル情報が表示されます。

例

#すべての LLDP ローカル情報を表示します。

<Sysname> display lldp local-information
Global LLDP local-information:
Chassis ID : 9820-44d2-3df8
System name : QX-W2300AC シリーズ
System description :
Comware Platform Software, Software Version 9.2.11
NEC QX-W2300AC シリーズ
System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge

System capabilities enabled : Bridge, Router, Customer Bridge

MED information:
Device class : Connectivity device
MED inventory information of master board:
HardwareRev : Ver.A
FirmwareRev : 3.03
SoftwareRev : Unknown
SerialNum : 210235A4AP9228Q0000F
Manufacturer name : NEC
Model name : QX-W2300AC シリーズ
Asset tracking identifier : Unknown
LLDP local-information of port 52[GigabitEthernet1/0/3]:
Port ID type : Interface name
Port ID : GigabitEthernet1/0/3
Port description : GigabitEthernet1/0/3 Interface
LLDP agent nearest-bridge management address:
Management address type : IPv4
Management address : 192.168.80.60
Management address interface type : IfIndex
Management address interface ID : Unknown
Management address OID : 0
LLDP agent nearest-nontpmr management address:
Management address type : IPv4
Management address : 192.168.80.61
Management address interface type : IfIndex
Management address interface ID : Unknown
Management address OID : 0
LLDP agent nearest-customer management address:
Management address type : IPv4
Management address : 192.168.80.62
Management address interface type : IfIndex
Management address interface ID : Unknown
Management address OID : 0
Link aggregation supported : Yes
Link aggregation enabled : Yes
Aggregation port ID : 52
Auto-negotiation supported : Yes
Auto-negotiation enabled : Yes
OperMau : Speed(1000)/Duplex(Full)
Power port class : PSE
PSE power supported : NO
PSE power enabled : NO

PSE pairs control ability ：NO
Power pairs ：Signal
Port power classification ：Class 0
Maximum frame size ：10000
PoE PSE power source ：Primary
Port PSE priority ：Critical
Port available power value：0.0 w

表 6-1 display lldp local-information コマンドの表示情報の説明

フィールド	説明
Global LLDP local-information	アプライアンスのグローバルLLDPローカル情報
Chassis ID	Chassis ID値は、このデバイスのブリッジMACアドレスです。
System name	システム名
System description	システムの説明
System capabilities supported	システムでサポートされている機能: • Bridge:スワップ機能がサポートされていることを示す • Router:ルーティング機能がサポートされていることを示す • Repeater:シグナルリレー機能がサポートされていることを示す • Telephone:電話機能がサポートされていることを示す • DocsisCableDevice:ケーブルデバイス機能がサポートされていることを示します。 • StationOnly:サイトのみの機能がサポートされていることを示します。 • Customer Bridge:カスタマーブリッジ機能をサポートしていることを示す • Service Bridge:サービスブリッジ機能がサポートされていることを示す • TPMR:デュアルポート MAC リレー機能のサポートを表明 • Other:上記以外の機能がサポートされていることを示します。

フィールド	説明
System capabilities enabled	システムの電源が入っている機能: • Bridge:スワップ機能がオンになっていることを示します。 • Router:ルーティング機能がオンになっていることを示します。 • Repeater:シグナルリレー機能がサポートされていることを示す • Telephone:電話機能がオンになっていることを示します。 • DocsisCableDevice:ケーブルデバイス機能がオンになっていることを示します。 • StationOnly:サイトのみの機能がオンになっていることを示します • Customer Bridge:ブリッジ機能がオンになっていることを示す • Service Bridge:サービスブリッジ機能がオンになっていることを示す • TPMR:デュアルポート MAC リレー機能がオンになっていることを示します。 • Other:上記以外の機能がオンになっていることを示します。
MED information	MEDデバイス関連情報
Device class	MEDデバイスタイプ: • Connectivity device:ネットワークデバイス • Class I:一般的なエンドデバイス、つまり LLDP ディスカバリサービスを必要とするすべてのエンドデバイスを表します。 • Class II:メディアエンドデバイス、すなわちメディアリテラシーを持つエンドデバイスを表し、そのリテラシーには一般的なエンドデバイスのリテラシーが含まれる。メディアフローをサポートするデバイス • Class III:通信端末機器、すなわちターゲットユーザの IP 通信システムを直接サポートする端末機器を表し、その能力には一般端末機器とメディア端末機器のすべての能力が含まれる。このデバイスは、ターゲットユーザによって直接使用されます。
MED inventory information of master board	ダッシュボードMED資産情報
HardwareRev	製品のハードウェアバージョン
FirmwareRev	製品のファームウェアバージョン

フィールド	説明
SoftwareRev	製品のソフトウェアバージョン
SerialNum	シリアル番号
Manufacturer name	製造メーカ
Model name	モジュール名
Asset tracking identifier	資産追跡ID
LLDP local-information of port 1	ポート1のLLDPローカル情報
Port ID type	ポートIDタイプ: • MAC address:MAC アドレス • Interface name:インタフェース名を表します。
Port ID	ポートID値。このデバイスのPort ID typeに応じて適切なタイプの値を取ります。
Port description	ポートの説明
LLDP agent nearest-bridge management address	LLDPnearestブリッジエージェントの管理アドレス
LLDP agent nearest-customer management address	LLDP最近のゲストブリッジエージェントの管理アドレス
LLDP agent nearest-nontpmr management address	LLDP最近の非TPMRブリッジエージェントの管理アドレス
Management address type	アドレスタイプの管理
Management address	管理アドレス
Management address interface type	管理アドレスが存在するインタフェースの符号化方式
Management address interface ID	管理アドレスインタフェースインデックス
Management address OID	アドレスオブジェクト識別子の管理
Link aggregation supported	ポートでリンクアグリゲーションがサポートされているかどうか
Link aggregation enabled	ポートでリンクアグリゲーションがオンになっているかどうか
Aggregation port ID	集約グループ内のそのメンバーポートの番号。リンク集約が有効になっていない場合は0。
Auto-negotiation supported	ポートでオートネゴシエーションがサポートされているかどうか
Auto-negotiation enabled	ポートでオートネゴシエーションが有効かどうか
OperMau	ポートの適応型レートおよびデュプレックスステータス
Power port class	PoEタイプ: • PSE (Power Sourcing Equipment、電源装置) • PD (Powered Device、受電設備)
PSE power supported	PSE電源はサポートされていますか?
PSE power enabled	PSE電源がオンになっているかどうか

フィールド	説明
PSE pairs control ability	給電方式は制御可能か
Power pairs	PoEポートのリモート電源モード: • Signal:信号線給電モードを示す • Spare:アイドルライン電源モードを示します。
Port power classification	PDのポート供給電力のクラスです。この表示は、PSEが供給できるPDの供給電力のクラスを表しており、PSE装置でない場合は未対応です。PSE装置でない場合は、”Class 0”を表示します。 • Class 0:レベル 0 を表します。 • Class 1:レベル 1 を表します。 • Class 2:レベル 2 を表します。 • Class 3:レベル 3 を表します。 • Class 4:レベル 4 を表します。
Maximum frame size	ポートでサポートされる最大フレーム長
PoE PSE power source	PSEで使用される電源タイプ: • Unknown:不明な電源タイプが使用されていることを示します • Primary:主電源が電源として使用されていることを示します。 • Backup:スタンバイパワーサプライが電源として使用されていることを示します。
PoE PD power source	PDで使用される電源タイプ: • Unknown:不明な電源タイプが使用されていることを示します • PSE:電源として PSE を使用することを示します。 • Local:電源としてローカル電源を使用することを示します。 • PSE and local:PSE およびローカル電源が電源として使用されていることを示します。
Port PSE priority	PSEのポートの電源プライオリティ: • Unknown:優先度が不明であることを示します。 • Critical:優先度がレベル 1 であることを示します。 • High:優先度がレベル 2 であることを示します。 • Low:優先度がレベル 3 であることを示します。
Port available power value	PSE上のポートで使用可能な電力、またはPD上のポートで必要な電力

6.1.2 display lldp neighbor-information

Syntax

display lldp neighbor-information [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }] [**verbose**]] | **list** [**system-name** *system-name*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定されたインタフェースがネイバーデバイスから受信した LLDP 情報を表示します。interface-type interface-number はインタフェースタイプとインタフェース番号を示します。このパラメータが指定されていない場合は、ネイバーデバイスによって受信されたすべてのインタフェースの LLDP 情報が表示されます。

agent:指定されたタイプの LLDP エージェントが受信した、ネイバーデバイスによって送信された LLDP 情報を表示します。このパラメータが指定されていない場合、すべてのタイプの LLDP エージェントが受信した、ネイバーデバイスによって送信された LLDP 情報が表示されます。

nearest-bridge:nearest ブリッジエージェントを表します。

nearest-customer:最近の顧客ブリッジエージェントを示します。

nearest-nontpmr:最近の非 TPMR ブリッジエージェントを示します。

verbose:ネイバーデバイスから送信された LLDP の詳細を表示します。このパラメータが指定されていない場合は、ネイバーデバイスから送信された LLDP プロファイルが表示されます。

list:ネイバーデバイスから送信された LLDP 情報をリストで表示します。

system-name *system-name*:指定されたネイバーデバイスから送信された LLDP 情報をリストで表示します。system-name はネイバーデバイスのシステム名で、1~255 文字の文字列です。このパラメータが指定されていない場合、すべてのネイバーデバイスから送信された LLDP 情報が一覧表示されます。

説明

display lldp neighbor-information コマンドは、ネイバーデバイスから送信された LLDP 情報を表示するために使用されます。

例

#すべてのインタフェースの最近ブリッジエージェントによって受信されたネイバーデバイスによって送信された LLDP の詳細を表示します(DCBX のバージョンが Standard であると仮定する)。

<Sysname> display lldp neighbor-information agent nearest-bridge verbose
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
LLDP Neighbor index : 1
Update time : 0 days, 0 hours, 1 minutes, 1 seconds
Chassis type : MAC address
Chassis ID : 000f-0055-0002
Port ID type : Interface name
Port ID : GigabitEthernet1/0/1
Time to live : 121
Port description : GigabitEthernet1/0/1 Interface
System name : QX-W2300AC シリーズ
System description :
Comware Platform Software, Software Version 9.1.058, 9.3.59
NEC QX-W2300AC シリーズ
System capabilities supported : Bridge, Router, Customer Bridge, Service Bridge
System capabilities enabled : Bridge, Router, Customer Bridge
Management address type : IPv4
Management address : 192.168.1.55
Management address interface type : IfIndex
Management address interface ID : Unknown
Management address OID : 0
Port VLAN ID(PVID): 1
Link aggregation supported : Yes
Link aggregation enabled : Yes
Aggregation port ID : 52
Auto-negotiation supported : Yes
Auto-negotiation enabled : Yes
OperMau : Speed(1000)/Duplex(Full)
Power port class : PD
PSE power supported : Yes
PSE power enabled : Yes
PSE pairs control ability : Yes
Power pairs : Signal
Port power classification : Class 0
Maximum frame size : 10000

#すべてのインタフェースすべてのタイプの LLDP エージェントが受信した、ネイバーデバイスによって送信された LLDP プロファイルを表示します。

<Sysname> display lldp neighbor-information

LLDP neighbor-information of port 52[GigabitEthernet1/0/3]:

LLDP agent nearest-bridge:

LLDP neighbor index : 3

ChassisID/subtype : 0011-2233-4400/MAC address

PortID/subtype : 000c-29f5-c71f/MAC address

Capabilities : Bridge, Router, Customer Bridge

LLDP neighbor index : 6

ChassisID/subtype : 0011-2233-4400/MAC address

PortID/subtype : 000c-29f5-c715/MAC address

Capabilities : None

CDP neighbor-information of port 52[GigabitEthernet1/0/3]:

LLDP agent nearest-bridge:

CDP neighbor index : 4

Chassis ID : SEP00260B5C0548

Port ID : Port 1

CDP neighbor index : 5

Chassis ID : 0011-2233-4400

Port ID : GigabitEthernet1/0/4

LLDP neighbor-information of port 52[GigabitEthernet1/0/3]:

LLDP agent nearest-nontpmr:

LLDP neighbor index : 6

ChassisID/subtype : 0011-2233-4400/MAC address

PortID/subtype : 000c-29f5-c715/MAC address

Capabilities : None

#タイプ別の LLDP プロキシすべてのネイバーデバイスからの LLDP 情報をリスト表示します。

<Sysname> display lldp neighbor-information list

Chassis ID : * -- --Nearest nontpmr bridge neighbor

-- --Nearest customer bridge neighbor

Default -- -- Nearest bridge neighbor

Local Interface	Chassis ID	Port ID	System Name
GE1/0/1	000f-e25d-ee91	GigabitEthernet1/0/1	System1

表 6-2 display lldp neighbor-information コマンドの表示情報の説明

フィールド	説明
LLDP agent nearest-bridge	LLDPデフォルト・エージェント、つまりnearestブリッジエージェント

フィールド	説明
LLDP agent nearest-customer	LLDP最近のクライアントブリッジエージェント
LLDP agent nearest-nontpmr	LLDP最近非TPMRブリッジエージェント
LLDP neighbor-information of port 1	ポート1で受信されたLLDPネイバー情報
LLDP Neighbor index	ネイバーインデックス
Update time	近隣情報の最新更新時刻
Chassis type	Chassis IDタイプ: • Chassis component:シェルフアセンブリを表します。 • Interface alias:インタフェースのエイリアスを表します。 • Port component:ポートコンポーネントを表します。 • MAC address:MAC アドレス • Network address (ipv 4):ネットワークアドレス(括弧内はアドレスタイプ) • Interface name:インタフェース名を表します。 • Locally assigned:ネイバーのカスタマイズ
Chassis ID	Chassis ID値は、ネイバーデバイスのChassis typeに基づいて適切なタイプの値を取ります。
Port ID type	ポートIDタイプ: • Interface alias:インタフェースのエイリアスを表します。 • Port component:ポートコンポーネントを表します。 • MAC address:MAC アドレス • Network Address (ipv 4):ネットワークアドレス(括弧内はアドレスタイプ) • Interface name:インタフェース名を表します。 • Agent circuit ID:エージェントのポーリング ID を示します。 • Locally assigned:ネイバーのカスタマイズ
Port ID	ポートID値は、ネイバーデバイスのPort ID typeに基づいて適切なタイプの値を取ります。
Time to live	ローカルのネイバー情報の存続時間
Port description	ポートの説明
System name	システム名
System description	システムの説明

フィールド	説明
System capabilities supported	システムでサポートされている機能: • Repeater:シグナルリレー機能がサポートされていることを示す • Bridge:スワップ機能がサポートされていることを示す • WlanAccessPoint:ワイヤレスアクセスポイント機能がサポートされていることを示します。 • Router:ルーティング機能がサポートされていることを示す • Telephone:電話機能がサポートされていることを示す • DocsisCableDevice:ケーブルデバイス機能がサポートされていることを示します。 • StationOnly:サイトのみの機能がサポートされていることを示します。 • Customer Bridge:カスタマーブリッジ機能をサポートしていることを示す • Service Bridge:サービスブリッジ機能がサポートされていることを示す • TPMR:デュアルポート MAC リレー機能のサポートを表明 • Other:上記以外の機能がサポートされていることを示します。

フィールド	説明
System capabilities enabled	システムの電源が入っている機能: • Repeater:シグナルリレー機能がオンになっていることを示す • Bridge:スワップ機能がオンになっていることを示します。 • WlanAccessPoint:ワイヤレスアクセスポイントがオンになっていることを示します。 • Router:ルーティング機能がオンになっていることを示します。 • Telephone:電話機能がオンになっていることを示します。 • DocsisCableDevice:ケーブルデバイス機能がオンになっていることを示します。 • StationOnly:サイトのみの機能がオンになっていることを示します • Customer Bridge:カスタマーブリッジ機能をサポートしていることを示す • Service Bridge:サービスブリッジ機能がサポートされていることを示す • TPMR:デュアルポート MAC リレー機能のサポートを表明 • Other:上記以外の機能がオンになっていることを示します。
Management address type	アドレスタイプの管理
Management address	管理アドレス
Management address interface type	管理アドレスインタフェースタイプ
Management address interface ID	管理アドレスインタフェースインデックス
Management address OID	アドレスオブジェクト識別子の管理
Port VLAN ID	ポートVLAN ID
Link aggregation supported	ポートでリンクアグリゲーションがサポートされているかどうか
Link aggregation enabled	ポートでリンクアグリゲーションがオンになっているかどうか
Aggregation port ID	集約グループ内のそのメンバーポートの番号。リンク集約が有効になっていない場合は0。
Auto-negotiation supported	ポートでオートネゴシエーションがサポートされているかどうか
Auto-negotiation enabled	ポートでオートネゴシエーションが有効かどうか

フィールド	説明
OperMau	ポートの適応型レートおよびデュプレックスステータス
Power port class	PoEタイプ: • PSE:電源装置を表します。 • PD:受電デバイスを表します。
PSE power supported	PSE電源はサポートされていますか?
PSE power enabled	PSE電源がオンになっているかどうか
PSE pairs control ability	給電方式は制御可能か
Power pairs	PoEポートのリモート電源モード: • Signal:信号線給電モードを示す • Spare:アイドルライン電源モードを示します。
Port power classification	PDのポート制御レベル: • Class 0:レベル 0 を表します。 • Class 1:レベル 1 を表します。 • Class 2:レベル 2 を表します。 • Class 3:レベル 3 を表します。 • Class 4:レベル 4 を表します。
Maximum frame size	ポートでサポートされる最大フレーム長
CDP neighbor-information of port 1	ポート1のCDPネイバー情報
CDP neighbor index	CDPネイバーインデックス
Chassis ID/subtype	Chassis ID値とChassis ID型
Port ID/subtype	Port ID値とPortID型

フィールド	説明
Capabilities	システムの電源が入っている機能: • Repeater:シグナルリレー機能がオンになっていることを示す • Bridge:スワップ機能がオンになっていることを示します。 • WlanAccessPoint:ワイヤレスアクセスポイント機能がオンになっていることを示します。 • Router:ルーティング機能がオンになっていることを示します。 • Telephone:電話機能がオンになっていることを示します。 • DocsisCableDevice:ケーブルデバイス機能がオンになっていることを示します。 • StationOnly:サイト機能のみを有効にし、他の機能と同時に表示しないことを示します • Other:上記リストにない他の機能がオンになっていることを示します。 • None:ネイバーが TLV を発行していないことを示します。
Local Interface	LLDP情報を受信するローカル・ポート
Chassis ID :*----Nearest nontpmr bridge neighbor #----Nearest customer bridge neighbor	*シンボル:このネイバーが最新の非TPMRブリッジエージェントタイプのネイバーであることを示します。 #記号:ネイバーが最も近いクライアントブリッジエージェントタイプのネイバーであることを示します。

6.1.3 display lldp statistics

Syntax

display lldp statistics [**global** | [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global:グローバル LLDP 統計情報を表示します。

interface *interface-type interface-number*:指定したインタフェースの LLDP 統計情報を表示します。interface-type interface-number はインタフェースタイプとインタフェース番号を示します。

agent:指定したタイプの LLDP エージェントの統計情報を表示します。このパラメータを指定しない場合、すべてのタイプの LLDP エージェントの統計が表示されます。

nearest-bridge:nearest ブリッジエージェントを表します。

nearest-customer:最近の顧客ブリッジエージェントを示します。

nearest-nontpmr:最近の非 TPMR ブリッジエージェントを示します。

説明

display lldp statistics コマンドを使用して、LLDP の統計情報を表示します。

パラメータを指定しない場合は、グローバルとインタフェースの両方の LLDP 統計情報が表示されます。

例

#グローバルおよびインタフェースの LLDP 統計情報を表示します。

<Sysname> display lldp statistics
LLDP statistics global information:
LLDP neighbor information last change time:0 days, 0 hours, 4 minutes, 40 seconds
The number of LLDP neighbor information inserted：1
The number of LLDP neighbor information deleted ：1
The number of LLDP neighbor information dropped ：0
The number of LLDP neighbor information aged out：1

LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
The number of LLDP frames transmitted ：0
The number of LLDP frames received ：0
The number of LLDP frames discarded ：0
The number of LLDP error frames ：0
The number of LLDP TLVs discarded ：0
The number of LLDP TLVs unrecognized ：0
The number of LLDP neighbor information aged out：0
The number of CDP frames transmitted ：0
The number of CDP frames received ：0
The number of CDP frames discarded ：0
The number of CDP error frames ：0

LLDP agent nearest-nontpmr:

The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0
The number of LLDP frames discarded : 0
The number of LLDP error frames : 0
The number of LLDP TLVs discarded : 0
The number of LLDP TLVs unrecognized : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted : 0
The number of CDP frames received : 0
The number of CDP frames discarded : 0
The number of CDP error frames : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0
The number of LLDP frames discarded : 0
The number of LLDP error frames : 0
The number of LLDP TLVs discarded : 0
The number of LLDP TLVs unrecognized : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted : 0
The number of CDP frames received : 0
The number of CDP frames discarded : 0
The number of CDP error frames : 0

#インタフェース GigabitEthernet1/0/1 の最近のゲストブリッジエージェントの LLDP 統計情報を表示します。

<Sysname> display lldp statistics interface gigabitethernet 1/0/1 agent nearest-customer
LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-customer:
The number of LLDP frames transmitted : 0
The number of LLDP frames received : 0
The number of LLDP frames discarded : 0
The number of LLDP error frames : 0
The number of LLDP TLVs discarded : 0
The number of LLDP TLVs unrecognized : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted : 0
The number of CDP frames received : 0
The number of CDP frames discarded : 0
The number of CDP error frames : 0

表 6-3 display lldp statistics コマンドの表示情報の説明

フィールド	説明
LLDP agent nearest-bridge	LLDPデフォルト・エージェント、つまりnearest ブリッジエージェント
LLDP agent nearest-customer	LLDP最近のクライアントブリッジエージェント
LLDP agent nearest-nontpmr	LLDP最近非TPMRブリッジエージェント
LLDP statistics global information	グローバルLLDP統計
LLDP neighbor information last change time	近隣情報の最終更新時刻
The number of LLDP neighbor information inserted	近隣情報の増加回数
The number of LLDP neighbor information deleted	ネイバー情報の削除回数
The number of LLDP neighbor information dropped	スペース不足によるネイバー情報の廃棄回数
The number of LLDP neighbor information aged out	ネイバー情報のエージング数
LLDP statistics Information of port 1	ポート1のLLDP統計
The number of LLDP frames transmitted	送信されたLLDPフレームの合計数
The number of LLDP frames received	受信したLLDPフレームの合計数
The number of LLDP frames discarded	ドロップされたLLDPフレームの合計数
The number of LLDP error frames	受信したエラーLLDPフレームの合計数
The number of LLDP TLVs discarded	廃棄されたLLDP TLVの合計数
The number of LLDP TLVs unrecognized	認識できないLLDP TLVの合計数
The number of LLDP neighbor information aged out	古いLLDPネイバー情報の合計数
The number of CDP frames transmitted	送信されたCDPフレームの合計数
The number of CDP frames received	受信したCDPフレームの合計数
The number of CDP frames discarded	廃棄されたCDPフレームの合計数
The number of CDP error frames	受信したエラーCDPフレームの合計数

6.1.4 display lldp status

Syntax

display lldp status [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースのLLDPステータス情報を表示します。interface-type interface-number はインタフェースタイプとインタフェース番号を示します。このパラメータを指定しない場合、LLDP 機能がオンになっているすべてのインタフェースの LLDP ステータス情報が表示されます。

agent:指定したタイプの LLDP エージェントのステータス情報を表示します。このパラメータを指定しない場合、すべてのタイプの LLDP エージェントのステータス情報が表示されます。

nearest-bridge:nearest ブリッジエージェントを表します。

nearest-customer:最近の顧客ブリッジエージェントを示します。

nearest-nontpmr:最近の非 TPMR ブリッジエージェントを示します。

説明

display lldp status コマンドを使用して、LLDP のステータス情報を表示します。

例

#グローバルおよびすべてのインタフェースの LLDP ステータス情報を表示します。

```
<Sysname> display lldp status
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 5
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 4 minutes, 40 seconds
Transmit interval          : 30s
Fast transmit interval     : 1s
Transmit max credit        : 5
Hold multiplier            : 4
Reinit delay               : 2s
Trap interval              : 5s
Fast start times           : 3

LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP        : Enable
Admin status               : TX_RX
Trap flag                  : No
MED trap flag              : No
Polling interval           : 0s
Number of LLDP neighbors   : 5
Number of MED neighbors    : 2
Number of CDP neighbors    : 0
```

Number of sent optional TLV : 12
Number of received unknown TLV : 5
Neighbor protection status : Port not protected

LLDP agent nearest-nontpmr:
Port status of LLDP : Enable
Admin status : TX_RX
Trap flag : No
MED trap flag : No
Polling interval : 0s
Number of LLDP neighbors : 5
Number of MED neighbors : 2
Number of CDP neighbors : 0
Number of sent optional TLV : 12
Number of received unknown TLV : 5
Neighbor protection status : Port not protected

LLDP agent nearest-customer:
Port status of LLDP : Enable
Admin status : TX_RX
Trap flag : No
MED trap flag : No
Polling interval : 0s
Number of LLDP neighbors : 5
Number of MED neighbors : 2
Number of CDP neighbors : 0
Number of sent optional TLV : 12
Number of received unknown TLV : 5
Neighbor protection status : Port not protected

表 6-4 display lldp status コマンドの表示情報の説明

フィールド	説明
Bridge mode of LLDP	LLDPブリッジモード: • service-bridge:サービスブリッジモードを表します。 • customer-bridge:カスタマーブリッジモード
LLDP agent nearest-bridge	LLDPデフォルト・エージェント、つまりnearestブリッジエージェント
LLDP agent nearest-customer	LLDP最近のクライアントブリッジエージェント
LLDP agent nearest-nontpmr	LLDP最近非TPMRブリッジエージェント
Global status of LLDP	LLDP機能がグローバルに有効かどうか
The current number of LLDP neighbors	現在のデバイスのLLDPネイバーの合計数

フィールド	説明
The current number of CDP neighbors	現在のデバイスのCDPネイバーの合計数
LLDP neighbor information last changed time	近隣情報の最終更新時刻
Transmit interval	LLDPメッセージの送信間隔
Hold multiplier	TTL乗数
Reinit delay	ポート初期化遅延時間
Transmit max credit	LLDPパケット速度制限トークンバケットの最大値
Trap interval	Trapメッセージの送信間隔
Fast start times	高速に送信されるLLDPメッセージの個数
LLDP status infomation of port 1	ポート1のLLDPステータス情報
Port status of LLDP	ポートでLLDP機能がオンになっているかどうか
Admin status	ポートLLDP動作モード: • TX_RX:LLDP メッセージの送信と受信の両方を表します。 • Rx_Only:LLDP メッセージのみを受信して送信しないことを示します。 • Tx_Only:LLDP メッセージのみが送信され、受信されないことを示します。 • Disable:LLDP メッセージを送信も受信もしないことを示します。
Trap Flag	LLDP Trap機能がオンになっているかどうか
MED trap flag	LLDP-MED Trap機能がオンになっているかどうか
Polling interval	ポーリング間隔:0はポーリング機能がオフになっていることを示します。
Number of neighbors	ポートLLDPネイバー数
Number of MED neighbors	ポートMEDネイバーデバイスの数
Number of CDP neighbors	ポートCDPネイバーデバイスの数
Number of sent optional TLV	ポートがLLDPメッセージで送信したオプションのTLVの合計数
Number of received unknown TLV	ポートがすべてのLLDPメッセージで受信した認識されないTLVの合計数

フィールド	説明
Neighbor protection status	ポートネイバー保護ステータス: • Port blocked (validation):ポートがブロックされていることを示します。ブロックの原因はネイバー識別情報の不一致です。 • Port blocked (aging):ネイバーのエージングタイムアウトがブロックの原因であることを示します。 • Port shutdown (aging):ネイバーエージングタイムアウトが原因でポートがダウンしていることを示します。 • Port not protected:ポートが保護されていないことを示します。

6.1.5 display lldp tlv-config

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースで送信可能なオプションの TLV 情報を表示します。interface-type interface-number はインタフェースタイプとインタフェース番号を示します。このパラメータが指定されていない場合は、すべてのインタフェースで送信可能なオプションの TLV 情報が表示されます。

agent:指定されたタイプの LLDP エージェントのオプションの TLV 情報を表示します。このパラメータが指定されていない場合は、すべてのタイプの LLDP エージェントのオプションの TLV 情報が表示されます。

nearest-bridge:nearest ブリッジエージェントを表します。

nearest-customer:最近の顧客ブリッジエージェントを示します。

nearest-nontpmr:最近の非 TPMR ブリッジエージェントを示します。

説明

display lldp tlv-config コマンドを使用して、インタフェースで送信可能なオプションの TLV 情報を表示します。

例

#インタフェース GigabitEthernet1/0/1 で送信できるオプションの TLV 情報を表示します。

<Sysname> display lldp tlv-config interface gigabitethernet 1/0/1

LLDP tlv-config of port 1[GigabitEthernet1/0/1]:

LLDP agent nearest-bridge:

NAME	STATUS	DEFAULT
Basic optional TLV:		
Port Description TLV	YES	YES
System Name TLV	YES	YES
System Description TLV	YES	YES
System Capabilities TLV	YES	YES
Management Address TLV	YES	YES
IEEE 802.1 extend TLV:		
Port VLAN ID TLV	YES	YES
Port And Protocol VLAN ID TLV	YES	YES
VLAN Name TLV	YES	YES
DCBX TLV	NO	NO
Link Aggregation TLV	YES	YES
Management VID TLV	YES	YES
IEEE 802.3 extend TLV:		
MAC-Physic TLV	YES	YES
Power via MDI TLV	YES	YES
Maximum Frame Size TLV	YES	YES
LLDP-MED extend TLV:		
Capabilities TLV	YES	YES
Location Identification TLV	NO	NO
Extended Power via MDI TLV	YES	YES
Inventory TLV	YES	YES

LLDP agent nearest-nontpmr:

NAME	STATUS	DEFAULT
Basic optional TLV:		
Port Description TLV	YES	NO
System Name TLV	YES	NO
System Description TLV	YES	NO
System Capabilities TLV	YES	NO
Management Address TLV	YES	NO
IEEE 802.1 extend TLV:		
Port VLAN ID TLV	YES	NO
Port And Protocol VLAN ID TLV	YES	NO
VLAN Name TLV	YES	NO
DCBX TLV	NO	NO
Link Aggregation TLV	YES	NO

```
  Management VID TLV                NO          NO
IEEE 802.3 extend TLV:
  MAC-Physic TLV                    YES         NO
  Power via MDI TLV                 YES         NO
  Maximum Frame Size TLV            YES         NO
LLDP-MED extend TLV:
  Capabilities TLV                  YES         NO
  Location Identification TLV       NO          NO
  Extended Power via MDI TLV        YES         NO
  Inventory TLV                     YES         NO

LLDP agent nearest-customer:
NAME                                STATUS      DEFAULT
Basic optional TLV:
  Port Description TLV              YES         YES
  System Name TLV                   YES         YES
  System Description TLV            YES         YES
  System Capabilities TLV           YES         YES
  Management Address TLV            YES         YES
IEEE 802.1 extend TLV:
  Port VLAN ID TLV                  YES         YES
  Port And Protocol VLAN ID TLV     YES         YES
  VLAN Name TLV                     YES         YES
  DCBX TLV                          NO          NO
  Link Aggregation TLV              YES         NO
  Management VID TLV                YES         YES
IEEE 802.3 extend TLV:
  MAC-Physic TLV                    YES         NO
  Power via MDI TLV                 YES         NO
  Maximum Frame Size TLV            YES         NO
LLDP-MED extend TLV:
  Capabilities TLV                  YES         YES
  Location Identification TLV       NO          NO
  Extended Power via MDI TLV        YES         NO
  Inventory TLV                     YES         YES
```

表 6-5 display lldp tlv-config コマンドの表示情報の説明

フィールド	説明
LLDP agent nearest-bridge	LLDP デフォルト・エージェント、つまりnearestブリッジエージェント
LLDP agent nearest-customer	LLDP最近のクライアントブリッジエージェント
LLDP agent nearest-nontpmr	LLDP最近非TPMRブリッジエージェント
LLDP tlv-config of port 1	ポート1で送信可能なオプションのTLVタイプ

フィールド	説明
NAME	TLV型
STATUS	ポートがパブリケーション指定タイプTLVを構成するかどうか
DEFAULT	ポートは、指定されたTLVタイプのデフォルトを発行します。
Basic optional TLV	ポートが送信できる基本TLVタイプ
Port Description TLV	ポート記述TLV
System Name TLV	システム名TLV
System Description TLV	システム記述TLV
System Capabilities TLV	システムコンピテンシーセットTLV
Management Address TLV	管理アドレスTLV
Congestion notification TLV	輻輳通知TLV
IEEE 802.1 extended TLV	ポートが送信できるIEEE 802.1組織定義のTLVタイプ
Port VLAN ID TLV	ポートVLAN ID TLV
Port And Protocol VLAN ID TLV	プロトコルVLAN ID TLV
VLAN Name TLV	VLAN名TLV
Management VID TLV	管理VLAN TLV
IEEE 802.3 extended TLV	ポートが送信できるIEEE 802.3組織定義のTLVタイプ
MAC-Physic TLV	ポートの物理属性TLV
Power via MDI TLV	電源容量TLV
Link Aggregation TLV	リンク集約TLV
Maximum Frame Size TLV	最大フレーム長TLV
LLDP-MED extend TLV	LLDP-MED TLV
Capabilities TLV	MEDコンピテンシーセットTLV
Network Policy TLV	ネットワークポリシーTLV
Location Identification TLV	ロケーションID TLV
Extended Power via MDI TLV	拡張電源TLV
Inventory TLV	資産情報TLVには、次のものが含まれます。 • Hardware Revision TLV:端末ハードウェアのバージョン • Firmware Revision TLV:端末デバイスのファームウェアバージョン • Software Revision TLV:端末ソフトウェアバージョン • Serial Number TLV:端末装置シリアル番号 • Manufacturer Name TLV:端末装置の製造業者名 • Model name TLV:端末デバイスのモジュール名 • Asset ID TLV:ディレクトリ管理と資産追跡のためのエンドデバイスの資産識別子
Energy-Efficient Ethernet TLV	Energy Efficient Ethernet TLV

6.1.6 lldp admin-status

Syntax

Layer 2 Ethernet interface view/Management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status**

Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **admin-status**

デフォルト

LLDPnearest ブリッジエージェントの動作モードは TxRx で、LLDP メッセージを送受信します。他のタイプの LLDP エージェントの動作モードは Disable です。つまり、LLDP メッセージは送信も受信もされません。

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent:指定したタイプの LLDP エージェントの動作モードを設定します。Ethernet Interface view/ Management Ethernet Interface view で、 Unspecified が指定されていない場合は、nearest ブリッジエージェントの動作モードが設定されています。

nearest-customer:最近の顧客ブリッジエージェントを示します。

nearest-nontpmr:最近の非 TPMR ブリッジエージェントを示します。

disable:動作モードが Disable で、 LLDP メッセージを送信も受信もしないことを示す。

rx:動作モードが Rx で、 LLDP メッセージのみを受信し送信しないことを示す。

tx:動作モードが Tx で、 LLDP メッセージのみを送受信しないことを示す。

txrx:動作モードが TxRx であり、 LLDP メッセージを送受信することを示す。

説明

lldp admin-status コマンドを使用して、LLDP の動作モードを設定します。

undo lldp admin-status コマンドを使用して、デフォルトの状態を復元します。

例

#設定インタフェース GigabitEthernet1/0/1 の最近のゲストブリッジエージェント LLDP の動作モードは Rx です。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx

6.1.7 lldp check-change-interval

Syntax

Layer 2 Ethernet interface view/Management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval** *interval*

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval**

Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **check-change-interval** *interval*

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **check-change-interval**

デフォルト

ポーリング機能がオフになっています。

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent:指定したタイプの LLDP エージェントのポーリング機能を設定します。Ethernet Interface view/ Management Ethernet Interface view で、 Unspecified が指定されていない場合は、nearest ブリッジエージェントの動作モードが設定されています。

nearest-customer:最近の顧客ブリッジエージェントを示します。

nearest-nontpmr:最近の非 TPMR ブリッジエージェントを示します。

interval:ポーリング間隔を秒単位で 1~30 の範囲で指定します。

説明

lldp check-change-interval コマンドは、ポーリング機能を有効にし、ポーリング間隔を設定するために使用します。

undo lldp check-change-interval コマンドは、ポーリング機能をオフにします。

例

#インタフェース GigabitEthernet1/0/1 のゲストブリッジエージェントでポーリングを有効にし、ポーリング間隔を 30 秒に設定します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30

6.1.8 lldp enable

Syntax

lldp enable

undo lldp enable

デフォルト

インタフェースの LLDP 機能がオンになっています。

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

lldp enable コマンドを使用して、インタフェースで LLDP 機能を有効にします。

undo lldp enable コマンドを使用して、インタフェースで LLDP 機能をオフにします。

LLDP 機能は、グローバルとインタフェースの両方で有効になっている場合にのみ有効になります。

例

#インタフェース GigabitEthernet1/0/1 で LLDP 機能をオフにします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo lldp enable

関連コマンド

- **lldp global enable**

6.1.9 lldp encapsulation snap

Syntax

Layer 2 Ethernet interface view/Management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation snap**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation**

Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **encapsulation snap**

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **encapsulation**

デフォルト

LLDP メッセージのカプセル化形式は Ethernet II です。

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent:指定したタイプの LLDP エージェントのカプセル化形式を設定します。Ethernet Interface view/ Management Ethernet Interface view で、 Unspecified が指定されていない場合は、nearest ブリッジエージェントの動作モードが設定されています。

nearest-customer:最近の顧客ブリッジエージェントを示します。

nearest-nontpmr:最近の非 TPMR ブリッジエージェントを示します。

説明

lldp encapsulation snap コマンドを使用して、LLDP メッセージのカプセル化形式を SNAP 形式に設定します。

undo lldp encapsulation コマンドを使用して、デフォルトの状態を復元します。

LLDP CDP メッセージのカプセル化形式は SNAP 形式のみで、Ethernet II 形式は使用できません。

例

#設定インタフェース GigabitEthernet1/0/1 で送信される LLDP メッセージのカプセル化形式は SNAP 形式です。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp encapsulation snap

6.1.10 lldp fast-count

Syntax

lldp fast-count *count*

undo lldp fast-count

デフォルト

LLDP メッセージを高速に送信する個数は 4 個である。

View

System view

定義済みユーザロール

network-admin

パラメータ

count:LLDP メッセージを高速に送信する個数を表し、 1~8 の範囲で値をとる。

説明

lldp fast-count コマンドは、高速に送信される LLDP メッセージの数を設定します。

undo lldp fast-count コマンドを使用して、デフォルトの状態を復元します。

例

#高速送信 LLDP メッセージの数を 5 個にする。

<Sysname> system-view
[Sysname] lldp fast-count 5

6.1.11 lldp global enable

Syntax

lldp global enable

undo lldp global enable

デフォルト

LLDP 機能はグローバルにオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

lldp global enable コマンドを使用して、LLDP 機能をグローバルに有効にします。

undo lldp global enable コマンドは、LLDP 機能をグローバルに停止するために使用します。

LLDP 機能は、グローバルとインタフェースの両方で有効になっている場合にのみ有効になります。

例

#LLDP 機能をグローバルに無効にします。

<Sysname> system-view
[Sysname] undo lldp global enable

関連コマンド

- **lldp enable**

6.1.12 lldp hold-multiplier

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

デフォルト

TTL 乗数は 4 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

value:TTL 乗数を表し、2~10 の値を取ります。

説明

lldp hold-multiplier コマンドを使用して、TTL 乗数を設定します。

undo lldp hold-multiplier コマンドを使用して、デフォルトの状態を復元します。

LLDP メッセージは Time To Live TLV の TTL 値を使用してネイバー情報のローカルデバイスでのエージングタイムを設定します。TTL=Min (65535、(TTL 乗数×LLDP メッセージ送信間隔+1))は 65535 と(TTL 乗数×LLDP メッセージ送信間隔+1)の最小値であるため、TTL 乗数を調整することでネイバーデバイスでのデバイス情報のエージングタイムを制御できます。

例

#TTL 乗数を 6 に設定します。

<Sysname> system-view
[Sysname] lldp hold-multiplier 6

関連コマンド

- **lldp timer tx-interval**

6.1.13 lldp management-address-format string

Syntax

Layer 2 Ethernet interface view/Management Ethernet interface view:

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **management-address-format string**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **management-address-format**

Layer 2 aggregate interface view:

lldp agent { **nearest-customer** | **nearest-nontpmr** } **management-address-format string**

undo lldp agent { **nearest-customer** | **nearest-nontpmr** } **management-address-format**

デフォルト

管理アドレスは、TLV の数値フォーマットでカプセル化されます。

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent:設定 TLV の LLDP エージェントタイプ管理アドレスのカプセル化形式を指定します。Layer 2 Ethernet interface view/Management Ethernet interface view で、指定されていない場合は、TLV の nearest ブリッジエージェントの管理アドレスのカプセル化形式を設定します。

nearest-customer:最近の顧客ブリッジエージェントを示します。

nearest-nontpmr:最近の非 TPMR ブリッジエージェントを示します。

説明

lldp management-address-format string コマンドは、TLV の管理アドレスを文字列形式でカプセル化するように設定します。

undo lldp management-address-format コマンドを使用して、デフォルトの状態を復元します。

ネイバーが管理アドレスを文字列形式で TLV にカプセル化する場合、ネイバーデバイスとの正常な通信を保証するために、ユーザはローカルデバイスでもカプセル化形式を文字列に変更できます。

LLDP メッセージでパブリッシュする IPv 6 形式の管理アドレスでは、数値形式のパッケージ形式のみがサポートされます。

例

#インタフェース GigabitEthernet1/0/1 の最後のゲストブリッジエージェントでの管理アドレスの設定 TLV のカプセル化形式は文字列形式です。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format string

6.1.14 lldp notification med-topology-change enable

Syntax

lldp notification med-topology-change enable

undo lldp notification med-topology-change enable

デフォルト

LLDP-MED Trap 機能がオフになっています。

View

Layer 2 Ethernet interface view

Management Ethernet interface view

定義済みユーザロール

network-admin

説明

lldp notification med-topology-change enable コマンドは、LLDP-MED Trap 機能を有効にするために使用します。

undo lldp notification med-topology-change enable コマンドは、LLDP-MED Trap 機能をオフにするために使用します。

例

#インタフェース GigabitEthernet1/0/1 で LLDP-MED Trap を有効にします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp notification med-topology-change enable

6.1.15 lldp timer notification-interval

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

デフォルト

LLDP Trap と LLDP-MED Trap のメッセージの送信間隔は、いずれも 30 秒である。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:LLDP Trap と LLDP-MED Trap のメッセージの送信間隔を示し、 53600 の範囲の値をとり、単位は秒である。

説明

lldp timer notification-interval コマンドは、LLDP Trap および LLDP-MED Trap 情報の送信間隔を設定するために使用します。

undo lldp timer notification-interval コマンドを使用して、デフォルトの状態を復元します。

例

#LLDP Trap および LLDP-MED Trap メッセージの送信間隔を 8 秒に設定します。

<Sysname> system-view
[Sysname] lldp timer notification-interval 8

6.1.16 lldp timer reinit-delay

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

デフォルト

インタフェース初期化の遅延時間は 2 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

delay:インタフェース初期化の遅延時間。1~10 の範囲で秒単位で指定できます。

説明

lldp timer reinit-delay コマンドを使用して、インタフェースの初期化の遅延時間を設定します。

undo lldp timer reinit-delay コマンドを使用して、デフォルトの状態を復元します。

例

#インタフェース初期化の遅延時間を 4 秒に設定します。

<Sysname> system-view
[Sysname] lldp timer reinit-delay 4

6.1.17 lldp timer tx-interval

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

デフォルト

LLDP メッセージの送信間隔は 30 秒である。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:LLDP メッセージの送信間隔を示し、 1~32768 の範囲の値をとり、単位は秒である。

説明

lldp timer tx-interval コマンドを使用して、LLDP メッセージの送信間隔を設定します。

undo lldp timer tx-interval コマンドを使用して、デフォルトの状態を復元します。

例

#LLDP メッセージの送信間隔を 20 秒に設定します。

<Sysname> system-view
[Sysname] lldp timer tx-interval 20

6.1.18 lldp tlv-enable

Syntax

Layer 2 Ethernet interface view:

- ブリッジエージェント LLDP インタフェースで許可されるパブリッシュの TLV タイプの設定

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id**

{ **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address* | **interface loopback** *interface-number*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** | **protocol-vlan-id** | **vlan-name** | **management-vid** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

- 最近の非 TPMR エージェント LLDP インタフェースで許可された発行 TLV タイプの設定

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

- 最近のゲストブリッジエージェント LLDP インタフェースで許可されているパブリッシュされた TLV タイプの設定

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **port-vlan-id** | **link-aggregation** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

Management Ethernet interface view:

lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* }&<1-10> | **elin-address** *tel-number* } } }

lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

undo lldp tlv-enable { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } | **dot3-tlv** { **all** | **mac-physic** | **max-frame-size** | **power** } | **med-tlv** { **all** | **capability** | **inventory** | **power-over-ethernet** | **location-id** } }

undo lldp agent { **nearest-nontpmr** | **nearest-customer** } **tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** | **management-address-tlv** [**ipv6**] [*ip-address*] } | **dot1-tlv** { **all** | **link-aggregation** } }

Layer 2 aggregate interface view:

lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

lldp tlv-enable dot1-tlv { **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **management-vid** [*mvlan-id*] }

undo lldp agent nearest-nontpmr tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp agent nearest-customer tlv-enable { **basic-tlv** { **all** | **management-address-tlv** [**ipv6**] [*ip-address*] | **port-description** | **system-capability** | **system-description** | **system-name** } | **dot1-tlv** { **all** | **port-vlan-id** } }

undo lldp tlv-enable dot1-tlv { **protocol-vlan-id** | **vlan-name** | **management-vid** }

デフォルト

Layer 2 Ethernet interface view:

- 最近のブリッジエージェントでは、Location-id TLV、Port And Protocol VLAN ID TLV、VLAN Name TLV、Management VLAN ID TLV 以外のすべてのタイプの TLV をパブリッシュできます。
- 最近の非 TPMR ブリッジエージェントは TLV を発行していません;
- 最近顧客ブリッジエージェントは基本 TLV および IEEE 802.1 組織定義 TLV をリリースすることを許可します。

Management Ethernet interface view:

- 最近のブリッジエージェントでは、Network Policy TLV 以外のすべてのタイプの TLV を発行できます。IEEE 802.1 組織定義の TLV は、Link Aggregation TLV のみをサポートします。
- 最近の非 TPMR ブリッジエージェントは TLV を発行していません;
- 最近ゲストブリッジエージェントは基本 TLV および IEEE 802.1 組織定義 TLV をリリースすることを許可します、ここで IEEE 802.1 組織定義 TLV は Link Aggregation TLV だけをサポートします。

Layer 2 aggregate interface view:

- 最近の非 TPMR ブリッジエージェントは TLV を発行していません;
- 最近ゲストブリッジエージェントは基本 TLV および IEEE 802.1 組織定義 TLV をリリースすることを許可します、IEEE 802.1 組織定義 TLV は Port And Protocol VLAN ID TLV、VLAN Name TLV および Management VLAN ID TLV だけをサポートします。

View

Layer 2 Ethernet interface view

Management Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

agent:設定指定されたタイプ LLDP エージェントが発行を許可する TLV タイプ。Layer 2 Ethernet interface view/Management Ethernet interface view の下で、指定されていない場合は、ブリッジエージェントが許可するリリースの TLV タイプを設定します。

nearest-customer:最近の顧客ブリッジエージェントを示します。

nearest-nontpmr:最近の非 TPMR ブリッジエージェントを示します。

all:指定されたタイプのすべてのオプション TLV をパブリッシュします。

- basic-tlv パラメータに all を指定すると、すべての基本 TLV のパブリッシュが許可されます。
- dot1-tlv パラメータに all を指定すると、すべての 802.1 組織定義 TLV の発行が許可されます。
- dot3-tlv パラメータに all を指定すると、すべての 802.3 組織定義 TLV の発行が許可されます。
- med-tlv パラメータに all を指定すると、location-id を除くすべてのオプションの LLDP-MED TLV のパブリッシュが許可されます。

basic-tlv:基本型 TLV を表します。

management-address-tlv [**ipv6**] [*ip-address* | **interface loopback** *interface-number*]:Management Address TLV であることを示す。ここで、ipv 6 は、LLDP メッセージで発行される管理アドレスが IPv 6 形式のアドレスであることを示しま

す。ip-address は、指定された IP アドレスが LLDP メッセージで発行された管理アドレスであることを示し、interface loopback interface-number は、指定された LoopBack インタフェースの IP アドレスが LLDP メッセージで発行された管理アドレスであることを示します。デフォルト値は次のとおりです。

- **lldp tlv-enable** コマンドの実行時:
  - Layer 2 Ethernet interface view で、ip-address パラメータが指定されていない場合、または指定された LoopBack インタフェースが存在しない場合、または LoopBack インタフェースに IPv4/IPv6 アドレスが設定されていない場合、発行された管理アドレスは、現在のインタフェースで許可されており、対応する VLAN インタフェースに IPv4/IPv6 アドレスが設定されていて、アップ状態にある最小 VLAN の IPv4/IPv6 アドレスになります。

    ipv 6 パラメータが指定されている場合、パブリケーションの管理アドレスは IPv 6 アドレスです。ipv 6 パラメータを指定しない場合、発行される管理アドレスは、対応する VLAN インタフェースの IP アドレス(IPv 4 アドレスと IPv 6 アドレスを含む)です。

    現在のインタフェースで許可されているすべての VLAN に対応する VLAN インタフェースで IPv4/IPv6 アドレスが設定されていないか、down 状態の場合、現在のインタフェースの MAC アドレスが発行されます。
  - Layer 2 aggregate interface view では、ip-address パラメータが指定されていない場合、発行された管理アドレスは、現在のインタフェースで許可されている、対応する VLAN インタフェース上で IPv4/IPv6 アドレスが設定されていて、アップ状態の最小 VLAN の IPv4/IPv6 アドレスになります。

    ipv 6 パラメータが指定されている場合、パブリケーションの管理アドレスは IPv 6 アドレスです。ipv 6 パラメータを指定しない場合、発行される管理アドレスは、対応する VLAN インタフェースの IP アドレス(IPv 4 アドレスと IPv 6 アドレスを含む)です。

    現在のインタフェースで許可されているすべての VLAN に対応する VLAN インタフェースで IPv4/IPv6 アドレスが設定されていないか、down 状態の場合、現在のインタフェースの MAC アドレスが発行されます。
- **undo lldp tlv-enable** コマンドの実行時:
  - Layer 2 Ethernet interface view/Management Ethernet interface view/Layer 2 aggregate interface view:

    ipv 6、ip-address、interface loopback interface-number パラメータを指定しない場合、TLV はパブリッシュされません。

    ipv 6、ip-address、および interface loopback interface-number パラメータを指定すると、TLV はデフォルト値でパブリッシュされます。

port-description:Port Description TLV を表します。

system-capability:System Capabilities TLV を表します。

system-description:System Description TLV を表します。

system-name:System Name TLV を表します。

dot1-tlv:IEEE 802.1 組織定義の TLV を表します。

port-vlan-id:Port VLAN ID TLV を表します。

protocol-vlan-id[*vlan-id*]:Port And Protocol VLAN ID TLV, vlan-id が発行する VLAN の VLAN ID であることを示します。範囲は 1~4094 で、デフォルト値はポートが属する VLAN の中で最も小さい VLAN ID です。

vlan-name[*vlan-id*]:VLAN Name TLV, vlan-id が発行する VLAN の VLAN ID であることを示します。範囲は 1~4094 で、デフォルト値はポートが属する VLAN の中で最も小さい VLAN ID です。vlan-id が指定されておらず、ポートが VLAN に参加していない場合、パブリッシュする VLAN はポートの PVID になります。

management-vid [*mvlan-id*]:Management VLAN ID TLV を表す。mvlan-id 管理 VLAN を発行する VLAN ID を 1~4094 の範囲の値で指定します。このパラメータが指定されていない場合は 0 が発行され、現在の LLDP agent に管理 VLAN が設定されていないことを示します。

link-aggregation:Link Aggregation TLV を表します。

dot3-tlv:IEEE 802.3 組織定義の TLV を表します。

mac-physic:MAC/PHY Configuration/Status TLV を表します。

max-frame-size:Maximum Frame Size TLV を表します。

power:Power Via MDI TLV および Power Stateful Control TLV を表します。

med-tlv:LLDP-MED TLV を表します。

capability:LLDP-MED Capabilities TLV を表します。

inventory:Hardware Revision TLV、Firmware Revision TLV、Software Revision TLV、Serial Number TLV、Manufacturer Name TLV、Model Name TLV、Asset ID TLV を表します。

power-over-ethernet:Extended Power-via-MDI TLV を表します。

location-id:Location Identification TLV を表します。

civic-address:Location Identification TLV がネットワークデバイスの共通アドレス情報をカプセル化することを示します。

device-type:デバイスタイプを示し、0~2 の値を取ります。0 はデバイスタイプ DHCP server、1 はデバイスタイプ Network device、2 はデバイスタイプ LLDP-MED Endpoint を表します。

country-code:国コードを表します。範囲は ISO 3166 を参照してください。

{ *ca-type ca-value* }&<1-10>:アドレス情報。ca-type はアドレス情報タイプで、0~255 の値を取ります。ca-value はアドレス情報を表す 1~250 文字の文字列である。&<1-10> は、前のパラメータが最大 10 回入力できることを示します。

elin-address:Location Identification TLV 緊急電話番号をカプセル化します。

tel-number:緊急電話番号を示す 10~25 文字の文字列。数字のみを使用できます。

説明

lldp tlv-enable コマンドを使用して、インタフェースで許可される TLV タイプを設定します。

undo lldp tlv-enable コマンドは、発行を禁止するインタフェースの TLV タイプを設定します。

集約インタフェースは、最近のブリッジエージェントをサポートしていません。

all パラメータを指定せずにこのコマンドを使用すると、一度に 1 つのタイプのオプション TLV のみを設定できます。この場合、コマンドを複数回使用して、各タイプの複数のオプション TLV を設定できます。

802.3 を発行していない組織が定義した MAC/PHY Configuration/Status TLV を発行する場合、LLDP-MED TLV は発行が許可されているかどうかに関係なく発行されません。LLDP-MED Capabilities TLV の発行が禁止されている場合、他の LLDP-MED TLV は発行が許可されているかどうかに関係なく発行されません。

IEEE 802.1 組織で定義された TLV の Port And Protocol VLAN ID TLV、VLAN Name TLV、および Management VLAN ID TLV は、最近のブリッジエージェント設定にのみ基づいていますが、その設定は最近の非 TPMR ブリッジエージェントと最近のゲストブリッジエージェントによって継承されます。

例

#設定インタフェース GigabitEthernet1/0/1 の最近のゲストブリッジエージェントは IEEE 802.1 組織によって定義される Link Aggregation オプション TLV をリリースすることを可能にします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv link-aggregation

6.1.19 reset lldp statistics

Syntax

reset lldp statistics [**interface** *interface-type interface number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*:ポートのタイプと番号を指定します。このオプションを指定しない場合、コマンドはすべてのポートの LLDP 統計情報をクリアします。

agent:エージェントタイプを指定します。エージェントタイプを指定しない場合、コマンドはすべての LLDP エージェントの LLDP 統計情報をクリアします。

nearest-bridge:最も近いブリッジエージェントを指定します。

nearest-customer:最も近いカスタマーブリッジエージェントを指定します。

nearest-nontpmr:最も近い非 TPMR ブリッジエージェントを指定します。

説明

オプションを指定しない場合、**reset lldp statistics** コマンドはすべてのポートの LLDP 統計情報をクリアしますが、グローバル LLDP 統計情報はクリアしません。

例

LLDP 統計情報をクリアします。
<Sysname> reset lldp statistics

関連コマンド

- **display lldp statistic**

目次

このセクションのページは **5-x-x** です。

7 章 レイヤ 2 フォワーディング 7-1
7.1 一般的なレイヤ 2 フォワーディングコマンド 7-1
7.1.1 display mac-forwarding statistics 7-1
7.1.2 reset mac-forwarding statistics 7-4
7.2 ファーストレイヤ 2 フォワーディングコマンド 7-5
7.2.1 display mac-forwarding cache ip 7-5
7.2.2 display mac-forwarding cache ip fragment 7-6

7章 レイヤ 2 フォワーディング

7.1 一般的なレイヤ2フォワーディングコマンド

7.1.1 display mac-forwarding statistics

Syntax

display mac-forwarding statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインターフェイスのレイヤ 2 転送統計情報を表示します。ここで、interface-type interface-number は指定されたインターフェイスタイプとインターフェイス番号です。このパラメータが指定されていない場合、レイヤ 2 転送グローバル統計が表示されます。

説明

display mac-forwarding statistics コマンドを使用して、レイヤ 2 転送統計情報を表示します。

例

#レイヤ 2 転送のグローバル統計を表示します。

<Sysname> display mac-forwarding statistics

```
Input:
  Sum:                  888          Unknown Unicast:    0
  Broadcast:            0            Multicast:          0
  Filtered:             0            STP discarded:      0
  Service dropped:      0            Source dropped:     0
  Unknown dropped:      0            Learning dropped:   0
  Blackhole dropped:    0            Suppress dropped:   0
  Source MAC dropped:0
Deliver:
  Sum:                  111          L2 protocol:        11
```

```
    Local MAC address: 100
Output:
    Sum:                666          Filtered:             0
    Blackhole dropped: 0             STP discarded:        0
    Service dropped:   0             Dest MAC dropped:     0
```

#インターフェイス GigabitEthernet1/0/1 のレイヤ 2 転送統計情報を表示します。

```
<Sysname> display mac-forwarding statistics interface gigabitethernet 1/0/1
GigabitEthernet1/0/1:
Input frames: 100       Output frames:100
Filtered:       0
```

表 7-1 display mac-forwarding statistics コマンドの表示情報の説明

フィールド	説明
Input	受信メッセージの統計。次の情報が含まれます。 ● Sum:受信されたEthernetフレームの合計数 ● Unknown unicast:不明なユニキャストMACアドレスを受信したEthernetフレームの数 ● Broadcast:受信したブロードキャスト宛先MACアドレスのイーサネットフレーム数 ● Multicast:受信したマルチキャスト宛先MACアドレスのイーサネットフレーム数 ● Filtered:802.1 Q Tagged VLANインインターフェイスフィルタリング規則に従ってフィルタリングされたイーサネットフレームの数 ● STP discarded:スパニングツリープロトコルがブロックされたためにドロップされた着信メッセージの数 ● Service dropped:着信トラフィックによってドロップされたイーサネットフレームの数 ● Source dropped:送信元MACアドレスがフルゼロ、マルチキャスト、またはブロードキャストアドレスであるためにドロップされたイーサネットフレームの数 ● Unknown dropped:送信元の不明なドロップが設定されたためにドロップされたイーサネットフレームの数 ● Learning dropped:MACアドレス学習数が上限に達した場合に、送信元MACアドレスがMACアドレステーブルにないメッセージの転送を禁止する機能により廃棄されるイーサネットのフレーム数 ● Blackhole dropped:送信元MACアドレスがブラックホールMACアドレスの場合に廃棄されるイーサネットフレームの数 ● Suppress dropped:不明なユニキャスト、ブロードキャスト、またはマルチキャストメッセージ抑制機能によってドロップされたイーサネットフレームの数 ● Source MAC dropped:送信元MACアドレスがドロップタイプMACアドレスの場合にドロップされるイーサネットフレームの数
Deliver	送信メッセージの統計。次の情報が含まれます。 ● Sum:アップストリームCPUによって処理された合計イーサネットフレーム数 ● L2 protocol:CPUにアップロードされるレイヤ2 プロトコルイーサネットのフレーム数 ● Local MAC address:宛先アドレスがローカルレイヤ3 VLANインターフェイスのMACアドレスであるイーサネットフレームの数

フィールド	説明
Output	ドロップされたメッセージの統計情報は次のとおりです。 ● Sum:送信されたEthernetフレームの合計数 ● Filtered:802.1 Q Tagged VLANアウトインターフェイスフィルタルールでフィルタリングされたイーサネットフレームの数 ● Blackhole dropped:宛先MACアドレスがブラックホールMACアドレスの場合に廃棄されるイーサネットフレームの数 ● STP discardedスパニングツリープロトコルがブロックされたためにドロップされたアウトバウンドメッセージの数 ● Service dropped:送信側トラフィックで廃棄されるイーサネットフレームの数 ● Dest MAC dropped:宛先MACアドレスのドロップを設定したためにドロップされたイーサネットフレームの数
GigabitEthernet1/0/1	インターフェイスGigabitEthernet1/0/1のレイヤ2 転送統計情報: ● Input frames:インターフェイスが受信するイーサネットフレームの数 ● Output frames:インターフェイスから送信されるイーサネットフレームの数 ● Filtered:インターフェイスでフィルタリングされた他のVLANのイーサネットフレームの数

7.1.2 reset mac-forwarding statistics

Syntax

reset mac-forwarding statistics

View

User view

定義済みユーザロール

network-admin

network-operator

説明

reset mac-forwarding statistics コマンドは、レイヤ 2 転送統計情報をクリアするために使用されます。

例

#レイヤ 2 転送統計情報をクリアします。

<Sysname> reset mac-forwarding statistics

7.2　ファーストレイヤ2フォワーディングコマンド

7.2.1 display mac-forwarding cache ip

Syntax

display mac-forwarding cache ip [*ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address:指定した IP アドレスの簡易転送テーブル情報を表示します。ip-address を指定しないと、すべての簡易転送テーブル情報が表示されます。

説明

display mac-forwarding cache ip コマンドは、IP 高速転送テーブル情報を表示するために使用されます。

例

#IP クイック転送テーブル情報を表示します。

<Sysname> display mac-forwarding cache ip

Total number of mac-forwarding entries: 2

SIP	SPort	DIP	DPort	Pro	Input_If	Output_If	VLAN
1.1.1.2	99	1.1.1.1	2048	1	GE1/0/1	GE1/0/2	2
1.1.1.1	98	1.1.1.2	2012	1	GE1/0/2	GE1/0/1	2

表 7-2　display mac-forwarding cache ip コマンドの表示情報の説明

フィールド	説明
Total number of mac-forwarding entries	高速転送エントリ数
SIP	ソースIPアドレス
SPort	ソースポート番号
DIP	宛先IPアドレス
DPort	宛先ポート番号
Pro	プロトコル番号

フィールド	説明
Input_If	着信インターフェイスのタイプとインターフェイス番号(「N/A」はインターフェイスが存在するが、このエクスプレスフォワーディングに着信インターフェイスが含まれていないことを示し、 「-」 はインターフェイスが存在しないことを示します。)
Output_If	アウトバウンドインターフェイスのタイプとインターフェイス番号(「N/A」はインターフェイスが存在するが、そのエクスプレスフォワーディングにインターフェイスが含まれていないことを示し、 「-」 はインターフェイスが存在しないことを示します。)
VLAN	VLAN ID

7.2.2 display mac-forwarding cache ip fragment

Syntax

display mac-forwarding cache ip fragment [*ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: IPv4 アドレスを指定します。IPv4 アドレスを指定しない場合、このコマンドはすべてのフラグメントの IPv4 高速転送エントリを表示します。

説明

フラグメントの IPv4 高速転送エントリを表示するには、**display mac-forwarding cache ip fragment** コマンドを使用します。

例

フラグメントの IPv4 高速転送エントリ情報を表示します。

<Sysname> display mac-forwarding cache ip fragment

Total number of fragment mac-forwarding entries: 2

SIP	SPort	DIP	DPort	Pro	Input_If	ID	VLAN
1.1.1.1	117	1.1.1.2	0	1	GE1/0/1	2828	1
1.1.1.2	110	1.1.1.1	67	17	GE1/0/2	2322	1

表 7-3　display mac-forwarding cache ip fragment コマンドの表示情報の説明

フィールド	説明
Total number of fragment mac-forwarding entries	フラグメント化されたメッセージの高速転送エントリ数
SIP	ソースIPアドレス
SPort	ソースポート番号
DIP	宛先IPアドレス
DPort	宛先ポート番号
Pro	プロトコル番号
Input_If	着信インターフェイスのタイプとインターフェイス番号(「N/A」はインターフェイスが存在するが、このエクスプレスフォワーディングに着信インターフェイスが含まれていないことを示し、 「-」 はインターフェイスが存在しないことを示します。)
ID	シャーディングIPメッセージID
VLAN	VLAN ID

目次

このセクションのページは **5-x-x** です。

8 章 ARP 8-1
8.1 ARP 設定コマンド 8-1
8.1.1 arp check enable 8-1
8.1.2 arp check log enable 8-2
8.1.3 arp mac-interface-consistency check enable 8-3
8.1.4 arp max-learning-num 8-4
8.1.5 arp static 8-5
8.1.6 arp timer aging 8-7
8.1.7 display arp 8-8
8.1.8 display arp ip-address 8-11
8.1.9 display arp timer aging 8-12
8.1.10 reset arp 8-12

8章 ARP

8.1 ARP設定コマンド

8.1.1 arp check enable

Syntax

arp check enable

undo arp check enable

デフォルト

ダイナミック ARP テーブルエントリのチェックがオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

arp check enable コマンドを使用して、ダイナミック ARP テーブルエントリのチェック機能を有効にします。

undo arp check enable コマンドを使用して、ダイナミック ARP テーブルエントリのチェック機能をオフにします。

ダイナミック ARP テーブルエントリチェック機能は、ARP メッセージの送信側 MAC アドレスがマルチキャスト MAC であるダイナミック ARP テーブルエントリをデバイスで学習できるかどうかを制御します。

ARP テーブルエントリの検査機能を有効にすると、ARP メッセージの送信側 MAC アドレスがマルチキャスト MAC であるダイナミック ARP テーブルエントリを学習したり、MAC アドレスがマルチキャスト MAC であるスタティック ARP テーブルエントリを手動で追加したりすることはできません。

ARP テーブルエントリのチェックをオフにすると、デバイスは、イーサネットの送信元 MAC アドレスがユニキャスト MAC であり、ARP メッセージの送信元 MAC アドレスがマルチキャスト MAC であるダイナミック ARP テーブルエントリを学習したり、MAC アドレスがマルチキャスト MAC であるスタティック ARP テーブルエントリを手動で追加したりできます。

例

#ダイナミック ARP テーブルエントリのチェックをオンにします。

<Sysname> system-view
[Sysname] arp check enable

8.1.2 arp check log enable

Syntax

arp check log enable

undo arp check log enable

デフォルト

デバイス ARP ログ情報機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

arp check log enable コマンド ARP ログ情報機能を有効にします。

undo arp check log enable コマンド ARP ログ情報機能を無効にします。

ARP ログを使用すると、管理者は問題の特定と解決を容易に行うことができます。ARP メッセージを処理するための情報が記録されます。これには、デバイスが ARP プロキシ機能を有効にしていない場合に、宛先 IP がデバイスのインタフェース IP アドレスでないことが含まれます。受信した ARP メッセージには送信元アドレスと受信インタフェースアドレスが含まれ、このメッセージは ARP 要求メッセージなどではありません。

デバイスによって生成された ARP ログ情報は、ログ情報の送信ルールと送信方向を決定するハブモジュールによって処理されます。ログ情報の送信設定についての詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*5 章 Info Center*”を参照してください。

デバイスが過剰な ARP ログ情報を出力してデバイスのパフォーマンスに影響を与えないようにするには、監査またはロケーションの問題を除き、この機能をオンにしないことをお勧めします。

例

#ARP ログメッセージ機能を有効にします。

<Sysname> system-view
[Sysname] arp check log enable

8.1.3 arp mac-interface-consistency check enable

Syntax

arp mac-interface-consistency check enable

undo arp mac-interface-consistency check enable

デフォルト

ARP テーブルエントリインタフェースと MAC アドレステーブルエントリインタフェースの整合性チェック機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

arp mac-interface-consistency check enable コマンドは、ARP テーブルエントリインタフェースと MAC アドレステーブルエントリインタフェースの整合性チェック機能を有効にします。

undo arp mac-interface-consistency check enable コマンドは、ARP テーブルエントリインタフェースと MAC アドレステーブルエントリインタフェースの整合性チェック機能を無効にするために使用します。

ネットワーク環境が不安定な場合、デバイスがユーザから送信されたメッセージを受信するインタフェースが変わることがあります。この時点で、デバイスはユーザの MAC アドレステーブルエントリのインタフェース情報を更新します。このユーザに対応する ARP テーブルエントリの発信側情報が更新されないため、この ARP テーブルエントリに一致するメッセージが不正なインタフェースから転送されます。この機能を有効にすると、ARP は定期的にユーザの ARP テーブルエントリの出力インタフェースと MAC アドレステーブルエントリの出力インタフェースが一致しているかどうかをチェックします。一致しない場合、ARP は当該ユーザの ARP 表エントリが記録した VLAN 内に ARP 要求メッセージを送信して探知し、かつ ARP 応答メッセージを受信したインタフェース情報を ARP 表エントリに更新し、ARP 表エントリのインタフェース出力情報がタイムリーに更新できることを保証し、あるユーザの ARP 表エントリのインタフェース出力と MAC アドレス表エントリのインタフェース出力が一致しない問題を解決する。

MAC アドレステーブル情報を表示するには、**display mac-address** コマンドを使用します。

例

#ARP テーブルエントリインタフェースと MAC アドレステーブルエントリインタフェースの整合性チェック機能を有効にします。

<Sysname> system-view

[Sysname] arp mac-interface-consistency check enable

関連コマンド

- **display mac-address (ネットワーク接続-MAC アドレステーブル)**

8.1.4 arp max-learning-num

Syntax

arp max-learning-num *max-number*

undo arp max-learning-num

デフォルト

このコマンドのデフォルト値は、max-number パラメータの最大範囲値です。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

max-number:インタフェースで学習できるダイナミック ARP テーブルエントリの最大数。

0～61440 の値が設定可能です。

説明

arp max-learning-num コマンドを使用して、ダイナミック ARP テーブルエントリの最大数を学習できるようにインタフェースを設定します。

undo arp max-learning-num コマンドを使用して、デフォルトの状態を復元します。

デバイスは、ARP プロトコルを使用してダイナミック ARP テーブルエントリを自動的に生成できます。一部のインタフェースの下のユーザが ARP リソースを過剰に消費するのを防ぐために、インタフェースが学習するダイナミック ARP テーブルエントリの最大数を設定することで制限できます。インタフェースが学習するダイナミック ARP テーブルエントリの数が設定された値に達すると、インタフェースはダイナミック ARP テーブルエントリを学習しなくなります。

インタフェースがダイナミック ARP テーブルエントリを学習できるように設定されている最大数が 0 時の場合、インタフェースはダイナミック ARP テーブルエントリを学習できません。

例

#設定 VLAN インタフェース 40 で学習できるダイナミック ARP テーブルエントリの最大数は 10 です。

<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40] arp max-learning-num 10

#設定インタフェース GigabitEthernet1/0/1 で学習できるダイナミック ARP テーブルエントリの最大数は 10 です。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp max-learning-num 10

#2 層集約インタフェースの設定 1 で学習できるダイナミック ARP テーブルエントリの最大数は 10 です。

<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] arp max-learning-num 10

8.1.5 arp static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]

undo arp *ip-address*

デフォルト

スタティック ARP テーブルエントリがありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address:ARP テーブルエントリの IP アドレス部分。

mac-address:ARP テーブルエントリの MAC アドレスの部分。形式は H-H-H です。

vlan-id:スタティック ARP テーブルエントリが属する VLAN。範囲は 1~4094 です。

interface-type interface-number:インタフェースタイプとインタフェース番号を指定します。

説明

スタティック ARP テーブルエントリを設定するには、**arp static** コマンドを使用します。

undo arp コマンドを使用して、ARP テーブルエントリを削除します。

スタティック ARP テーブルエントリを手動で設定して維持することで、エージングが発生せず、ダイナミック ARP テーブルエントリで上書きされないため、通信のセキュリティが向上します。

スタティック ARP テーブルエントリは、短いスタティック ARP テーブルエントリと長いスタティック ARP テーブルエントリに分けられます。

- 解決された短いスタティック ARP エントリは、解決されたアウトインタフェースの状態が down になったり、vlan-id に対応する VLAN および VLAN インタフェースが削除されたりするなどの外部イベントにより、未解決の状態に戻ります。
- 長いスタティック ARP テーブルエントリの場合、デバイスの現在の状態に応じて、有効な状態と無効な状態があります。無効な状態は、ARP テーブルエントリの IP アドレスがローカル IP アドレスと競合しているか、ARP テーブルエントリの IP アドレスと同じネットワークセグメント上にあるデバイス上のインタフェースアドレスがないことが原因です。無効な状態の長いスタティック ARP テーブルエントリは、メッセージ転送を指示できません。

vlan-id interface-type interface-number パラメータを指定する場合は、次の点に注意してください。

- interface-type interface-number は、イーサネットインタフェースまたは集約インタフェースのいずれかです。
- vlan-id に対応する VLAN および VLAN インタフェースが存在し、インタフェース interface-type interface-number がこの VLAN に属している必要があります。
- vlan-id 対応する VLAN インタフェースの IP アドレスは、ip-address と同じセグメントに属している必要があります。
- vlan-id 対応する VLAN および VLAN インタフェースが削除されると、長いスタティック ARP テーブルエントリが削除されます。

例

#IP アドレス 202.38.10.2、対応する MAC アドレス 00 e0-fc01-0000、および VLAN 10 に属するインタフェース GigabitEthernet1/0/1 に対応する出力インタフェースを持つ長いスタティック ARP テーブルエントリを設定します。

<Sysname> system-view
[Sysname] arp static 202.38.10.2 00 e0-fc01-0000 10 gigabitethernet 1/0/1

関連コマンド

- **display arp**
- **reset arp**

8.1.6 arp timer aging

Syntax

arp timer aging { *aging-minutes* | **second** *aging-seconds* }

undo arp timer aging

デフォルト

ダイナミック ARP テーブルエントリのエージングタイムは 20 分です。

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-minutes:ダイナミック ARP テーブルエントリの経過時間を分単位で 1~1440 の範囲で指定します。

second *aging-seconds*:ダイナミック ARP エントリのエージングタイムを秒単位で 5~86400 の範囲で指定します。

説明

ダイナミック ARP テーブルエントリのエージングタイムを設定するには、**arp timer aging** コマンドを使用します。

undo arp timer aging コマンドを使用して、デフォルトの状態を復元します。

ネットワークの変化に対応するには、ARP テーブルを常に更新する必要があります。ARP テーブル内のダイナミック ARP テーブルエントリは常に有効ではありません。各レコードには有効期限があり、有効期限に達しても更新されないレコードは ARP テーブルから削除されます。有効期限はエージングタイムと呼ばれます。エージングタイムに達する前にレコードが更新された場合は、エージングタイムが再計算されます。

プロキシ ARP 機能を設定したら、ダイナミック ARP テーブルエントリのエージングタイムを短縮して、無効なダイナミック ARP テーブルエントリをできるだけ早く無効にし、デバイスに送信されてデバイスが転送できないメッセージを減らして、無効なダイナミック ARP テーブルエントリをできるだけ早く削除する必要があります。

例

#ダイナミック ARP テーブルエントリのエージングタイムを 10 分に設定します。

<Sysname> system-view
[Sysname] arp timer aging 10

#ダイナミック ARP テーブルエントリのエージングタイムを 200 秒に設定します。

<Sysname> system-view

[Sysname] arp timer aging second 200

関連コマンド

- **display arp timer aging**

8.1.7 display arp

Syntax

display arp [[**all** | **dynamic** | **static**] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての ARP テーブルエントリを表示します。

dynamic:ダイナミック ARP テーブルエントリを表示します。

static:スタティック ARP テーブルエントリを表示します。

vlan vlan-id:指定した VLAN の ARP テーブルエントリを表示します。vlan-id の値の範囲は 1~4094 です。

interface *interface-type interface-number*:指定したインタフェースの ARP テーブルエントリを表示します。interface-type interface-number インタフェースタイプとインタフェース番号を指定するために使用します。このパラメータを指定しない場合は、すべてのインタフェースの ARP テーブルエントリが表示されます。

count:ARP テーブルエントリの数を表示します。

verbose:ARP テーブルエントリの詳細を表示します。

説明

display arp コマンドを使用して、ARP テーブルエントリを表示します。

このコマンドを使用して、IP アドレス、MAC アドレス、VLAN ID、発信インタフェース、テーブルエントリタイプ、エージングタイムなどの情報を含む、スタティックなダイナミック ARP テーブルエントリを表示します。

例

#すべての ARP テーブルエントリの情報を表示します。

<Sysname> display arp all

```
  Type: S-Static    D-Dynamic    O-Openflow    R-Rule   I-Invalid
IP address      MAC address     VLAN/VSI name Interface              Aging Type
1.1.1.1         02e0-f102-0023 1              GE1/0/1                --    S
1.1.1.2         00e0-fc00-0001 12             GE1/0/2                960   D
1.1.1.3         00e0-fe50-6503 vsi1           Tunnel1                960   D
```

#すべての ARP テーブルエントリの詳細を表示します。

<Sysname> display arp all verbose

```
  Type: S-Static    D-Dynamic    O-Openflow    R-Rule   I-Invalid
IP address      : 1.1.1.1          MAC address    : 02e0-f102-0023
Type            : Static           Aging          : --
Interface       : GE1/0/1          SVLAN/CVLAN    : 1/--
VPN instance    : --
Link ID         : --
Service instance: --
VXLAN ID        : --
VSI name        : --
VSI interface   : --

IP address      : 1.1.1.2          MAC address    : 00e0-fc00-0001
Type            : Dynamic          Aging          : 960 seconds
Interface       : GE1/0/2          SVLAN/CVLAN    : 12/--
VPN instance    : --
Link ID         : --
Service instance: --
VXLAN ID        : --
VSI name        : --
VSI interface   : --

IP address      : 1.1.1.3          MAC address    : 00e0-fe50-6503
Type            : Dynamic          Aging          : 960 seconds
Interface       : Tunnel1          SVLAN/CVLAN    : 12/--
VPN instance    : --
Link ID         : --
Service instance: --
VXLAN ID        : --
VSI name        : vsi1
VSI interface   : --
```

#すべての ARP テーブルエントリの数を表示します。

<Sysname> display arp all count

```
 Total number of entries : 3
```

表 8-1 display arp コマンドの表示情報の説明

フィールド	説明
IP address	ARPテーブルエントリのIPアドレス
MAC address	ARPテーブルエントリのMACアドレス
VLAN/VSI name	ARPテーブルエントリが属するパブリックネットワークVLAN ID (テーブルエントリタイプが静的な場合、「--」は、未解決の短い静的ARPテーブルエントリを表します。ARPテーブルエントリのインタフェースがVLANに属していない場合は、「--」も表示されます。)
Interface	ARPテーブルエントリに対応する出力インタフェース(テーブルエントリタイプが静的な場合、「--」は、未解決の短い静的ARPテーブルエントリを表します。)
Aging	ARPテーブルエントリのエージングタイム。スタティックARPテーブルエントリの場合、このフィールドにはエージングタイムがないことを示す「--」の値が入ります。ダイナミックARPテーブルエントリの値は次のとおりです。 • 秒単位のエージング時間の値 • 「--」は、経過時間が不明であることを示します。
Type	ARPテーブルエントリタイプ。値は次のとおりです。 • D は動的 • S は静的 • O は OpenFlow を表します。 • R は Rule を表します • 無効な表現
SVLAN/CVLAN	ARPエントリが属するパブリックネットワークVLAN ID/プライベートネットワークVLAN ID (テーブルエントリタイプが静的な場合、「--」は、未解決の短い静的ARPテーブルエントリを表します。ARPテーブルエントリのインタフェースがVLANに属していない場合は、「--」も表示されます。)
VPN instance	(未サポート) VPNインスタンス名、「--」は、対応するARPが設定されていないVPNインスタンスを示します。
Link ID	(未サポート) ARPテーブルエントリがVSIに属していない場合は、「--」と表示されます。
Service instance	Ethernetサービスインスタンス:ARPテーブルエントリでレイヤ2 Ethernetインタフェースまたはレイヤ2集約インタフェース上のEthernetサービスインスタンスが指定されていない場合は、「--」と表示されます。
VXLAN ID	(未サポート) VXLAN ID、VNI (VXLAN ネットワーク識別子)とも呼ばれ、「--」はこのアイテムがどのVXLANにも属していないことを意味します。
VSI name	(未サポート) ARPエントリのVSI名「--」は、エントリがVSIに属していないことを示します。
VSI interface	(未サポート) VSIに関連付けられたVSI仮想インタフェース。VSIに関連付けられたVSI仮想インタフェースが指定されていない場合は「--」

フィールド	説明
Total number of entries	ARPテーブルエントリ数

関連コマンド

- **arp static**
- **reset arp**

8.1.8 display arp ip-address

Syntax

display arp *ip-address* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address:指定した IP アドレスの ARP テーブルエントリを表示します。

verbose:ARP テーブルエントリの詳細を表示します。

説明

display arp ip-address コマンドを使用して、指定した IP アドレスの ARP テーブルエントリを表示します。

このコマンドを使用すると、IP アドレス、MAC アドレス、VLAN ID、発信インタフェース、テーブルエントリタイプ、エージングタイムなどの情報を含む、指定した IP アドレスの ARP テーブルエントリの詳細を表示できます。

例

#IP アドレス 20.1.1.1 の ARP テーブルエントリに関する情報を表示します。

<Sysname> display arp 20.1.1.1

Type:S-StaticD-DynamicO-OpenflowR-RuleI-Invalid

IP addressMAC addressVLAN/VSI name InterfaceAging Type

20.1.1.100 e0-fc00-0001 N/A----S

関連コマンド

- **arp static**

- **reset arp**

8.1.9 display arp timer aging

Syntax

display arp timer aging

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display arp timer aging コマンドを使用して、ダイナミック ARP テーブルエントリの経過時間を表示します。

arp timer aging コマンドで設定されたエージングタイムに関係なく、このコマンドは秒単位のエージングタイムを表示します。

例

#ダイナミック ARP テーブルエントリのエージングタイムを表示します。

<Sysname> display arp timer aging
Current ARP aging time is 1200 seconds

上記の情報は、ダイナミック ARP テーブルエントリのデフォルトのエージングタイムが 1200 秒であることを示しています。

関連コマンド

- **arp timer aging**

関連コマンド

- **arp user-ip-conflict record enable**

8.1.10 reset arp

Syntax

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all:すべての ARP テーブルエントリをクリアすることを示します。

dynamic:ダイナミック ARP テーブルエントリをクリアすることを示します。

static:スタティック ARP テーブルエントリをクリアします。

interface *interface-type interface-number*:指定したインタフェースの ARP テーブルエントリをクリアします。interface-type interface-number インタフェースのタイプと番号を指定するために使用します。このパラメータを指定しない場合は、すべてのインタフェースの ARP テーブルエントリがクリアされます。

説明

reset arp コマンドを使用して、ARP テーブルエントリをクリアします。

 注意

このコマンドを実行すると、デバイス上の既存の ARP テーブルエントリがクリアされるため、外部トラフィックがローカルエリアネットワーク上のユーザーに到達できなくなる可能性があります。

例

#スタティック ARP テーブルエントリをクリアします。

<Sysname> reset arp static

関連コマンド

- **arp static**
- **display arp**

目次

このセクションのページは **5-x-x** です。

9 章 Gratuitous ARP 9-1
9.1 Gratuitous ARP 設定コマンド 9-1
9.1.1 arp ip-conflict log prompt 9-1
9.1.2 arp send-gratuitous-arp 9-2
9.1.3 gratuitous-arp mac-change retransmit 9-3
9.1.4 gratuitous-arp-learning enable 9-4
9.1.5 gratuitous-arp-sending enable 9-5

9章 Gratuitous ARP

9.1 Gratuitous ARP設定コマンド

9.1.1 arp ip-conflict log prompt

Syntax

arp ip-conflict log prompt

undo arp ip-conflict log prompt

デフォルト

ソース IP アドレス競合プロンプト機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

arp ip-conflict log prompt コマンドを使用して、送信元 IP アドレスの競合に関するプロンプトを表示します。

undo arp ip-conflict log prompt コマンドは、送信元 IP アドレスの競合に関するプロンプト機能をオフにするために使用します。

デバイスは、他のデバイスから送信された ARP メッセージを受信した後、そのメッセージ内の送信元 IP アドレスが自分の IP アドレスと同じであることを検出すると、現在の送信元 IP アドレス競合通知機能の状態に基づいて、次の処理を実行します。

- 送信元 IP アドレスの競合通知機能がオフの場合、デバイスは、対応する ARP 応答を受信するまで IP アドレスの競合を通知しないで、競合を確認するために Gratuitous ARP メッセージを送信します。
- 送信元 IP アドレスの競合に関するプロンプトが表示されている場合は、IP アドレスの競合に関するプロンプトが表示されます。

例

#送信元 IP アドレスの競合に関するプロンプトをデバイスでオンにします。

<Sysname> system-view
[Sysname] arp ip-conflict log prompt

9.1.2 arp send-gratuitous-arp

Syntax

arp send-gratuitous-arp [**interval** *interval*]

undo arp send-gratuitous-arp

デフォルト

Gratuitous ARP パケットの定期送信は無効になっています。

View

VLAN Interface view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: GratuitousARP メッセージを送信する間隔。ミリ秒単位で 200~200000 の値をとり、デフォルト値は 2000 です。

説明

arp send-gratuitous-arp コマンドは、インタフェースで GratuitousARP 送信機能をオンにするために使用されます。

undo arp send-gratuitous-arp コマンドは、GratuitousARP 送信機能をオフにするために使用されます。

この機能は、インタフェースに IP アドレスがあり、インタフェースのデータリンク層の状態がアップしている場合にのみ、インタフェースで有効になります。

この機能は、送信側インタフェースのプライマリ IP アドレスまたは手動で設定されたセカンダリ IP アドレスに対してのみ、不要な ARP 要求を送信できます。プライマリ IP アドレスは手動または自動で設定できますが、セカンダリ IP アドレスは手動で設定する必要があります。

不要な ARP パケットの送信間隔を変更した場合、設定は次の送信間隔で有効になります。

次のいずれかの条件が存在する場合、不要な ARP パケットの送信間隔は設定された間隔よりもはるかに長くなることがあります。

- この機能は、複数のインタフェースで有効になっています。
- 各インタフェースには、複数のセカンダリ IP アドレスが設定されています。
- 上記のケースでは、小さい送信間隔が設定されています。

例

300 ミリ秒ごとに Gratuitous ARP パケットを送信するには、VLAN インタフェース 2 を有効にします。

<Sysname> system-view

[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp send-gratuitous-arp interval 300

9.1.3 gratuitous-arp mac-change retransmit

Syntax

gratuitous-arp mac-change retransmit *times* **interval** *seconds*

undo gratuitous-arp mac-change retransmit

デフォルト

デバイスのインタフェース MAC アドレスが変更されると、インタフェースは 1 回だけ Gratuitous ARP メッセージを送信します。

View

System view

定義済みユーザロール

network-admin

パラメータ

times:1~10 の範囲で Gratuitous ARP メッセージが再送信された回数。

interval *seconds*:Gratuitous ARP メッセージを再送信する間隔。*seconds* は、1~10 の範囲の値を秒単位で取得します。

説明

gratuitous-arp mac-change retransmit コマンドを使用して、インタフェースの MAC アドレスが変更された場合に Gratuitous ARP メッセージを再送信する回数と間隔を設定します。

undo gratuitous-arp mac-change retransmit コマンドを使用して、デフォルトの状態を復元します。

デバイスの MAC アドレスが変更されると、デバイスは、Gratuitous ARP メッセージを使用して、変更された MAC アドレスを他のデバイスにアドバタイズします。現在、Gratuitous ARP メッセージには再送信メカニズムがないため、他のデバイスは Gratuitous ARP メッセージを受信できない場合があります。この問題を解決するには、インタフェースの MAC アドレスが変更された場合に、インタフェースが Gratuitous ARP メッセージを再送信する回数と間隔を設定して、他のデバイスが Gratuitous ARP メッセージを受信できるようにします。

このコマンドを実行すると、設定された送信回数に達するまで、デバイスは指定された間隔で Gratuitous ARP メッセージを再送信します。

例

#設定インタフェースの MAC アドレスが変更されると、インタフェースは 5 秒間隔で 3 回の Gratuitous ARP メッセージを再送信します。

<Sysname> system-view
[Sysname] gratuitous-arp mac-change retransmit 3 interval 5

9.1.4 gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

デフォルト

Gratuitous ARP メッセージの学習機能がオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-learning enable コマンドを使用して、Gratuitous ARP メッセージの学習機能を有効にします。

undo gratuitous-arp-learning enable コマンドを使用して、Gratuitous ARP メッセージ学習機能を無効にします。

Gratuitous ARP メッセージの学習を有効にすると、デバイスは、受信した Gratuitous ARP メッセージに含まれる情報に基づいて、自身が保持する ARP テーブルを変更します(ARP テーブルエントリの新規作成または更新)。

Gratuitous ARP メッセージのラーニングを無効にすると、デバイスは受信した Gratuitous ARP メッセージに基づいて新しい ARP テーブルエントリを作成しませんが、既存の対応する ARP テーブルエントリは更新されます。Gratuitous ARP メッセージを使用して新しい ARP テーブルエントリを作成したくない場合は、Gratuitous ARP メッセージ学習機能をオフにして、ARP テーブルエントリのリソースを節約できます。

例

#Gratuitous ARP メッセージの学習機能を有効にします。

<Sysname> system-view
[Sysname] gratuitous-arp-learning enable

9.1.5 gratuitous-arp-sending enable

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

デフォルト

デバイスが同じネットワークセグメント以外の ARP 要求を受信したときに、Gratuitous ARP メッセージを送信する機能はオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-sending enable コマンドを使用すると、デバイスが同じネットワークセグメント以外のARP要求を受信したときに、Gratuitous ARP メッセージを送信できます。

undo gratuitous-arp-sending enable コマンドは、デバイスが同じネットワークセグメント以外の ARP 要求を受信した場合に、Gratuitous ARP メッセージを送信する機能を無効にするために使用します。

例

送信元 IP アドレスが異なるサブネット上にある ARP 要求を受信したときに、デバイスが不要な ARP パケットを送信できないようにします。

<Sysname> system-view
[Sysname] undo gratuitous-arp-sending enable

目次

このセクションのページは **5-x-x** です。

10 章 Proxy ARP 10-1
10.1 Proxy ARP 設定コマンド 10-1
10.1.1 display local-proxy-arp 10-1
10.1.2 display proxy-arp 10-2
10.1.3 local-proxy-arp enable 10-2
10.1.4 proxy-arp enable 10-4

10章 Proxy ARP

ユーザアイソレーション機能とプロキシ ARP 機能を同時に使用する場合、プロキシ ARP はサービステンプレートに割り当てている VLAN では使用できません。

10.1 Proxy ARP設定コマンド

10.1.1 display local-proxy-arp

Syntax

display local-proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースのローカルプロキシ ARP のステータスを表示します。interface-type interface-number インタフェースタイプとインタフェース番号を指定します。このパラメータを指定しない場合は、すべてのインタフェースのローカルプロキシ ARP のステータスが表示されます。

説明

display local-proxy-arp コマンドを使用して、ローカルプロキシ ARP のステータスを表示します。

このコマンドを使用して、ローカルプロキシ ARP がオン(enabled)かオフ(disabled)かを確認します。

例

#VLAN インタフェース 2 のローカルプロキシ ARP ステータスを表示します。

<Sysname> display local-proxy-arp interface vlan-interface 2

Interface Vlan-interface2

Local Proxy ARP status:enabled

関連コマンド

- **local-proxy-arp enable**

10.1.2 display proxy-arp

Syntax

display proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type Interface-number*:指定したインタフェースのプロキシ ARP のステータスを表示します。interface-type interface-number インタフェースタイプとインタフェース番号を指定するために使用します。このパラメータを指定しない場合は、すべてのインタフェースのプロキシ ARP のステータスが表示されます。

説明

display proxy-arp コマンドを使用して、プロキシ ARP のステータスを表示します。

このコマンドを使用して、プロキシ ARP がオン(enabled)かオフ(disabled)かを確認します。

例

#VLAN インタフェース 2 のプロキシ ARP ステータスを表示します。

<Sysname> display proxy-arp interface vlan-interface 2

Interface Vlan-interface2

Proxy ARP status:disabled

関連コマンド

- **proxy-arp enable**

10.1.3 local-proxy-arp enable

Syntax

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

undo local-proxy-arp enable

デフォルト

ローカルプロキシ ARP 機能がオフになっています。

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ip-range *start-ip-address* **to** *end-ip-address*:指定された IP アドレス範囲に対するローカルプロキシ ARP を設定します。start-ip-address は、開始 IP アドレスです。end-ip-address は終了 IP アドレスを表します。start-ip-address は end-ip-address 以下でなければなりません。

説明

local-proxy-arp enable コマンドを使用して、ローカルプロキシ ARP 機能を有効にします。

undo local-proxy-arp enable コマンドを使用して、ローカルプロキシ ARP 機能をオフにします。

ARP 要求が、あるネットワーク上のホストから、同じ物理ネットワーク上ではなく同じネットワークセグメント上の別のホストに送信された場合、そのホストに接続されているプロキシ ARP 対応デバイスがその要求に応答することができます(Proxy ARP)。

プロキシ ARP 機能は、分離された物理ネットワークをブロックし、あたかも同じ物理ネットワーク上にあるかのように使用します。

プロキシ ARP は、通常のプロキシ ARP とローカルプロキシ ARP に分かれています。

- 通常のプロキシ ARP は、デバイスの異なるレイヤ 3 インタフェースにそれぞれ接続され、同じブロードキャストドメインに存在しないホストと通信したい場合に使用します。
- ローカルプロキシ ARP は、デバイスの同じレイヤ 3 インタフェースに接続されていて、同じブロードキャストドメインに存在しないホストと通信したい場合に使用します。

このコマンドを複数回実行して、異なる IP アドレス範囲を設定してローカルプロキシ ARP を実行すると、最後に実行したコマンドが有効になることに注意してください。

例

#VLAN インタフェース 2 でネイティブプロキシ ARP 機能を有効にします。

<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable

#VLAN インタフェース 2 でネイティブプロキシ ARP 機能を有効にし、ARP プロキシを実行する IP アドレスの範囲を指定します。

<Sysname> system-view

[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20

関連コマンド

- **display local-proxy-arp**

10.1.4 proxy-arp enable

Syntax

proxy-arp enable

undo proxy-arp enable

デフォルト

プロキシ ARP 機能がオフになっています。

View

VLAN interface view

定義済みユーザロール

network-admin

説明

proxy-arp enable コマンドを使用して、プロキシ ARP 機能を有効にします。

undo proxy-arp enable コマンドは、プロキシ ARP 機能を停止するために使用します。

ARP 要求が、あるネットワーク上のホストから、同じ物理ネットワーク上ではなく同じネットワークセグメント上の別のホストに送信された場合、そのホストに接続されているプロキシ ARP 対応デバイスがその要求に応答することができます(Proxy ARP)。

プロキシ ARP 機能は、分離された物理ネットワークをブロックし、あたかも同じ物理ネットワーク上にあるかのように使用します。

プロキシ ARP は、通常のプロキシ ARP とローカルプロキシ ARP に分かれています。

- 通常のプロキシ ARP は、デバイスの異なるレイヤ 3 インタフェースにそれぞれ接続され、同じブロードキャストドメインに存在しないホストと通信したい場合に使用します。
- ローカルプロキシ ARP は、デバイスの同じレイヤ 3 インタフェースに接続されていて、同じブロードキャストドメインに存在しないホストと通信したい場合に使用します。

例

#VLAN インタフェース 2 でプロキシ ARP をオンにします。

<Sysname> system-view
[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] proxy-arp enable

関連コマンド

- **display proxy-arp**

目次

このセクションのページは **5-x-x** です。

11 章 IP アドレス 11-1
11.1 IP アドレス設定コマンド 11-1
11.1.1 display ip interface 11-1
11.1.2 display ip interface brief 11-4
11.1.3 ip address 11-6

11章 IP アドレス

11.1 IPアドレス設定コマンド

11.1.1 display ip interface

Syntax

display ip interface [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type:インタフェースのタイプを指定します。

interface-number:インタフェース番号を指定します。

説明

display ip interface コマンドを使用して、IP に関連するレイヤ 3 インタフェースの設定と統計情報を表示します。

display ip interface コマンドを使用して、インタフェースで送受信されたユニキャストメッセージの数、バイト数、マルチキャストメッセージの数、インタフェースで受信された無効な TTL メッセージの数、ICMP メッセージの数など、レイヤ 3 インタフェースの IP 関連の設定と統計情報を表示します。

表示されたメッセージの送受信状況を分析することで、ネットワークが攻撃されているかどうかや、攻撃の発生源となっている可能性があるかどうかを判断できます。

インタフェースタイプのみを指定すると、そのタイプのすべてのインタフェースに関する情報が表示されます。パラメータを指定しない場合は、レイヤ 3 すべてのインタフェースの IP 関連の設定と統計情報が表示されます。

例

#VLAN インタフェース 10 の IP 関連の設定と統計情報を表示します。

<Sysname> display ip interface vlan-interface 10

Vlan-interface10 current state: DOWN

Line protocol current state: DOWN

Internet Address is 1.1.1.1/8 Primary

Broadcast address: 1.255.255.255
The Maximum Transmit Unit: 1500 bytes
input packets：0, bytes：0, multicasts：0
output packets：0, bytes：0, multicasts：0
TTL invalid packet number: 0
ICMP packet input number: 0
Echo reply: 0
Unreachable: 0
Source quench: 0
Routing redirect: 0
Echo request: 0
Router advert: 0
Router solicit: 0
Time exceed: 0
IP header bad: 0
Timestamp request: 0
Timestamp reply: 0
Information request: 0
Information reply: 0
Netmask request: 0
Netmask reply: 0
Unknown type: 0

表11-1 display ip interface コマンドの表示情報の説明

フィールド	説明
current state	インタフェースの現在の物理状態、考えられる状態、および意味は次のとおりです。 • Administratively DOWN:インタフェースが shutdown コマンドでシャットダウンされたことを示します。つまり、管理状態はシャットダウンです。 • DOWN:このインタフェースの管理状態は ON ですが、物理状態は OFF です(接続されていないか、回線が故障している可能性があります) • UP:インタフェースの管理状態と物理状態の両方がオンです。

フィールド	説明
Line protocol current state	インタフェースデータリンク層プロトコルの状態、考えられる状態、および意味は次のとおりです。 • DOWN:インタフェースのデータリンク層プロトコルの状態がオフであることを示します • UP:インタフェースのデータリンク層プロトコルステータスがオンであることを示します。 • UP (spoofing):インタフェースのプロトコル状態はスプーフィング ON である。つまり、インタフェースのリンク層プロトコル状態は ON を示しているが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性がある。
Internet Address	インタフェースのIPアドレス。IPアドレスの後に次のパラメータを指定できます。 • Primary:手動で構成されたプライマリ IP アドレスを示します。 • Sub:手動で構成されたスレーブ IP アドレスを表します。 • Unnumbered:IP アドレスを借用していることを示します。 • DHCP-Allocated:DHCP が動的に IP アドレスを割り当てることを示します。 • BOOTP-Allocated:IP アドレスが BOOTP に動的に割り当てられていることを示します。 • Mad:MAD IP アドレスを表します。
Broadcast address	インタフェースが存在するネットワークセグメントのブロードキャストアドレス
The Maximum Transmit Unit	バイト単位のインタフェースの最大転送単位
input packets、bytes、multicasts output packets、bytes、multicasts	インタフェースで送受信されるすべてのメッセージの数、バイト数、およびマルチキャストメッセージの数(デバイスが起動すると、この情報の統計が開始されます。)
TTL invalid packet number	インタフェースで受信された無効なTTLメッセージの数(デバイスが起動すると、この情報の統計が開始されます。)

フィールド	説明
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	次のメッセージを含む、インタフェースで受信されたICMPメッセージの合計数(デバイスが起動すると、この情報の統計が開始されます。)。 • エコー応答メッセージ • 到達不能メッセージ • ソース抑制メッセージ • 経路リダイレクトメッセージ • エコー要求メッセージ • ルーター広告メッセージ • ルーター要求メッセージ • タイムアウトメッセージ • IP ヘッダーのエラー・メッセージ • タイムスタンプ要求メッセージ • タイムスタンプ応答メッセージ • 情報要求メッセージ • 情報応答メッセージ • マスク要求メッセージ • マスク応答メッセージ • 不明なタイプのメッセージ

関連コマンド

- **display ip interface brief**
- **ip address**

11.1.2 display ip interface brief

Syntax

display ip interface [*interface-type* [*interface-number*]] **brief** [**description**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type:指定したタイプのインタフェースの IP 基本設定情報を表示します。このパラメータが指定されていない場合は、レイヤ 3 すべてのインタフェースの IP 関連の簡単な情報が表示されます。

interface-number:指定したインタフェースの IP 基本設定情報を表示します。このパラメータが指定されていない場合は、そのタイプのすべてのレイヤ 3 インタフェースの IP 関連の簡単な情報が表示されます。

description:インタフェースの完全な説明情報を表示します。このパラメータが指定されていない場合は 16 文字まで、16 文字を超える場合は最初の 14 文字と「...」が表示されます。

説明

display ip interface brief コマンドを使用して、IP に関連するレイヤ 3 インタフェースの簡単な情報を表示します。

display ip interface brief コマンドを使用すると、レイヤ 3 インタフェースの IP 関連の簡単な情報を表示できます。これには、インタフェースの物理層とリンク層のプロトコルステータス、IP アドレス、説明などが含まれます。

例

#VLAN インタフェースの基本設定情報を表示します。

```
<Sysname> display ip interface vlan-interface brief
*down: administratively down
(s): spoofing  (l): loopback
Interface                Physical Protocol IP Address      Description
Vlan10                   down     down     6.6.6.1         Link to CoreRo...
Vlan2                    down     down     7.7.7.1         --
<Sysname> display ip interface vlan-interface brief description
*down: administratively down
(s): spoofing  (l): loopback
Interface                Physical Protocol IP Address      Description
Vlan10                   down     down     6.6.6.1         Link to CoreRouter
Vlan2                    down     down     7.7.7.1         --
```

表11-2　display ip interface brief コマンドの表示情報の説明

フィールド	説明
*down:administratively down	インタフェースが管理down状態になると、shutdownコマンドでシャットダウンされます。

フィールド	説明
(s) :spoofing	インタフェースのスプーフィング属性、つまりインタフェースのリンク層プロトコルステータスはupと表示されますが、実際には対応するリンクがないか、または対応するリンクが永続的ではなくオンデマンドで確立されている可能性があります。
Interface	インタフェースの名前
Physical	インタフェースの物理状態、考えられる状態、および意味は次のとおりです。 • *down:インタフェースが shutdown コマンドでシャットダウンされたことを示します。つまり、管理状態がシャットダウンです。 • down:インタフェースの管理ステータスはオンですが、物理ステータスはオフです(接続されていないか、回線が故障している可能性があります)。 • up:このインタフェースの管理状態と物理状態の両方がオンになっています
Protocol	インタフェースのリンク層プロトコルの状態、考えられる状態、および意味は次のとおりです。 • down:このインタフェースのプロトコルステータスはオフです • down (l) :インタフェースのプロトコルステータスは loopback down です。 • up:このインタフェースのプロトコルステータスはオンです • up (l) :このインタフェースのプロトコルステータスは loopback up です。 • up (s) :このインタフェースのプロトコルステータスは spoofing up です。
IP Address	インタフェースのIPアドレス(構成されていない場合は「--」)
Description	インタフェースの説明情報(構成されていない場合は「--」)

関連コマンド

- **display ip interface**
- **ip address**

11.1.3 ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* | *mask* } [**sub**]]

デフォルト

インタフェースの IP アドレスが設定されていません。

View

Interface viewInterface view

定義済みユーザロール

network-admin

パラメータ

ip-address:10 進ドット表記のインタフェースの IP アドレス。

mask-length:サブネットマスクの長さ。マスク内の連続する 「1」 の数。範囲は 1~31 で、インタフェースが LoopBack の場合は 1~32 です。

mask:インタフェース IP アドレスに対応するサブネットマスク。ドット付き 10 進表記です。

sub:このアドレスがインタフェースのスレーブ IP アドレスであることを示します。

説明

ip address コマンドを使用して、インタフェースの IP アドレスを設定します。

undo ip address コマンドを使用して、インタフェースの IP アドレスを削除します。

ip address コマンドを使用して、インタフェースの IP アドレスを設定します。デバイスの各インタフェースには複数の IP アドレスを設定できます。1 つはプライマリ IP アドレスで、残りはスレーブ IP アドレスです。一般に、1 つのインタフェースには 1 つのプライマリ IP アドレスを設定するだけで済みますが、1 つのインタフェースで複数のサブネット間の通信を可能にするために、インタフェースにセカンダリ IP アドレスを設定する必要がある場合もあります。

1 つのインタフェースには 1 つのプライマリ IP アドレスしか設定できません。同じインタフェースで複数回このコマンドを実行してプライマリ IP アドレスを設定すると、最後に実行したコマンドが有効になります。

インタフェースが BOOTP または DHCP を使用して他のインタフェースの IP アドレスを動的に取得または借用するように設定されている場合、そのインタフェースにからの IP アドレスを設定することはできません。

undo ip address コマンドにパラメータを指定しないと、インタフェースのすべての IP アドレスが削除されます。undo ip address ip-address {mask |mask-length }プライマリ IP アドレスを削除することを示します。undo ip address ip-address {mask |mask-length } sub は指定されたスレーブ IP アドレスを削除することを示します。

同じインタフェースのマスターIP アドレスとスレーブ IP アドレスを同じセグメントにすることはできますが、異なるインタフェース間、マスターインタフェースとそのサブイ

ンタフェース間、同じマスターインタフェースの下の異なるサブインタフェース間の IP アドレスを同じセグメントにすることはできません。

例

#VLAN インタフェース 10 のプライマリ IP アドレスを 129.12.0.1、セカンダリ IP アドレスを 202.38.160.1、サブネットマスクを 255.255.255.0 に指定します。

<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address 129.12.0.1 255.255.255.0
[Sysname-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub

関連コマンド

- **display ip interface**
- **display ip interface brief**

目次

このセクションのページは **5-x-x** です。

12 章 DHCP 共通 12-1
12.1 DHCP 共通コマンド 12-1
12.1.1 dhcp dscp 12-1
12.1.2 dhcp enable 12-2
12.1.3 dhcp select 12-2

12章 DHCP 共通

12.1 DHCP共通コマンド

12.1.1 dhcp dscp

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

デフォルト

DHCP サーバまたは DHCP リレーが DHCP メッセージを送信する DSCP プライオリティは 56 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value:DHCP メッセージの DSCP 優先度。範囲は 0~63 です。

説明

dhcp dscp コマンドを使用して、DHCP サーバまたは DHCP リレーが DHCP メッセージを送信する DSCP プライオリティを設定します。

undo dhcp dscp コマンドを使用して、デフォルトの状態を復元します。

DSCP 優先度は、メッセージ自体の優先度を表し、メッセージ転送の優先度を決定する。DSCP 優先度の設定値が大きいほど、メッセージの優先度が高くなります。

例

#DHCP サーバまたは DHCP リレーが送信する DHCP メッセージの DSCP プライオリティを 30 に設定します。

<Sysname> system-view
[Sysname] dhcp dscp 30

12.1.2 dhcp enable

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

デフォルト

DHCP サービスが停止しています。

View

System view

定義済みユーザロール

network-admin

説明

dhcp enable コマンドを使用して、DHCP サービスを有効にします。

undo dhcp enable コマンドは、DHCP サービスを停止するために使用します。

その他の関連する DHCP 設定は、DHCP サービスが有効になっている場合にのみ有効になります。

DHCP サーバと DHCP リレーを設定する場合は、最初に DHCP サービスを有効にする必要があります。

例

#DHCP サービスを有効にします。

<Sysname> system-view
[Sysname] dhcp enable

12.1.3 dhcp select

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

デフォルト

インタフェースは DHCP サーバモードで動作し、DHCP クライアントからの DHCP メッセージを受信すると、DHCP サーバのアドレスプールからアドレスなどのパラメータが割り当てられます。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

relay DHCP リレーモードで動作するようにインタフェースを設定します。

server:DHCP サーバモードで動作するようにインタフェースを設定します。

説明

dhcp select コマンドは、DHCP サーバまたは DHCP リレーモードで動作するようにインタフェースを設定するために使用します。

undo dhcp select コマンドは、DHCP サーバまたは DHCP リレーモードでのインタフェースの動作を解除するために使用されます。

インタフェースが DHCP サーバモードから DHCP リレーモードに切り替わった後、デバイスは IP アドレスバインディング情報を削除せず、対応する認証 ARP テーブルエントリも削除しません。これらのテーブルエントリは、DHCP リレーによって新しく生成された ARP テーブルエントリと競合する可能性があります。したがって、インタフェースを DHCP サーバモードから DHCP リレーモードに切り替える前に、**reset dhcp server ip-in-use** コマンドを使用して既存の IP アドレスバインディング情報をクリアすることをお勧めします。

例

#設定 VLAN インタフェース 2 は DHCP リレーモードで動作します。

<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp select relay

関連コマンド

- **dhcp relay always-unicast**
- **dhcp server request-ip-address check**
- **dhcp smart-relay enable**
- **reset dhcp server ip-in-use**

目次

このセクションのページは **5-x-x** です。

13 章 DHCP サーバ 13-1
13.1 DHCP サーバ設定コマンド 13-1
13.1.1 address range 13-1
13.1.2 bims-server 13-2
13.1.3 bootfile-name 13-3
13.1.4 class option-group 13-4
13.1.5 dhcp class 13-5
13.1.6 dhcp option-group 13-6
13.1.7 dhcp server apply ip-pool 13-7
13.1.8 dhcp server forbidden-ip 13-8
13.1.9 dhcp server ip-pool 13-10
13.1.10 dhcp server ping packets 13-10
13.1.11 dhcp server ping timeout 13-12
13.1.12 dhcp server relay information enable 13-13
13.1.13 display dhcp server conflict 13-14
13.1.14 display dhcp server expired 13-15
13.1.15 display dhcp server free-ip 13-17
13.1.16 display dhcp server ip-in-use 13-18
13.1.17 display dhcp server pool 13-21
13.1.18 display dhcp server statistics 13-24
13.1.19 dns-list 13-27
13.1.20 domain-name 13-28
13.1.21 expired 13-28
13.1.22 forbidden-ip 13-30
13.1.23 gateway-list 13-31
13.1.24 if-match 13-32
13.1.25 nbns-list 13-35
13.1.26 netbios-type 13-36
13.1.27 network 13-37
13.1.28 next-server 13-39
13.1.29 option 13-40
13.1.30 reset dhcp server conflict 13-42
13.1.31 reset dhcp server expired 13-43
13.1.32 reset dhcp server ip-in-use 13-43
13.1.33 reset dhcp server statistics 13-44
13.1.34 snmp-agent trap enable dhcp server 13-45

13.1.35 static-bind 13-46
13.1.36 tftp-server domain-name 13-48
13.1.37 tftp-server ip-address 13-49
13.1.38 voice-config 13-50

13章 DHCP サーバ

13.1 DHCPサーバ設定コマンド

13.1.1 address range

Syntax

address range *start-ip-address end-ip-address*

undo address range

デフォルト

動的に割り当てられた IP アドレス範囲が構成されていません。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address:動的に割り当てられた範囲の開始 IP アドレス。

end-ip-address:範囲の終了 IP アドレスを動的に割り当てます。

説明

address range コマンドを使用して、アドレスプールに動的に割り当てられる IP アドレスの範囲を設定します。

undo address range コマンドを使用して、デフォルトの状態を復元します。

アドレスプールによって動的に割り当てられる IP アドレスの範囲がこのコマンドで設定されていない場合は、アドレスプールの **network** コマンドで指定されたネットワークセグメントアドレスを DHCP クライアントに割り当てることができます。アドレスプールによって動的に割り当てられる IP アドレス範囲がこのコマンドで設定されている場合、クライアントに割り当てるアドレスは、このコマンドで指定された IP アドレス範囲からのみ選択できます。

address range コマンドを設定した後、**network secondary** コマンドを使用してネットワークセグメントからアドレスプールを設定することはできなくなりました。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

address range コマンドで指定されたアドレス範囲は、**network** コマンドで指定されたネットワークセグメント範囲内である必要があります。ネットワークセグメント範囲外のアドレスは割り当てられません。

例

#設定アドレスプール 1 動的に割り当てられるアドレスの範囲は 192.168.8.1~192.168.8.150 です。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 1
[Sysname-dhcp-pool-1] network 192.168.8.1 mask 255.255.255.0
[Sysname-dhcp-pool-1] address range 192.168.8.1 192.168.8.150
```

関連コマンド

- **class**
- **dhcp class**
- **display dhcp server pool**
- **network**

13.1.2 bims-server

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*

undo bims-server

デフォルト

DHCP アドレスプールが構成されていない DHCP クライアントに割り当てられた BIMS サーバ情報。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*:BIMS サーバの IP アドレスを指定します。

port *port-number*:BIMS サーバのポート番号を指定します。port-number はポート番号で、範囲は 1~65534 です。

cipher:キーを暗号化テキストとして設定します。

simple:暗号化されたテキストとして保存されるキーをクリアテキストで設定します。

string:キー文字列。大文字と小文字が区別されます。平文鍵は 1~16 文字の文字列、暗号文鍵は 1~53 文字の文字列である。DHCP クライアントは、 BIMS サーバの情報を取得した後、 BIMS サーバと通信する際に、共有鍵を用いて配信されるメッセージを暗号化し、メッセージの安全性を保証する。

説明

bims-server コマンドを使用して、DHCP アドレスプールが DHCP クライアントに割り当てる BIMS サーバの IP アドレス、ポート、および共有キー情報を設定します。

undo bims-server コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#DHCP アドレスプールの設定 0 DHCP クライアントに割り当てられた BIMS サーバの IP アドレスは 1.1.1.1、ポート番号は 80、共有キーは aabbcc です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc

関連コマンド

- **display dhcp server pool**

13.1.3 bootfile-name

Syntax

bootfile-name { *bootfile-name* | *url* }

undo bootfile-name

デフォルト

DHCP クライアントが使用する起動ファイル名またはリモート起動ファイルの HTTP 形式の URL が設定されていません。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

bootfile-name:起動ファイル名。1~63 文字の文字列で、大文字と小文字が区別されます。

url:リモート起動ファイルの HTTP 形式の URL。1~63 文字の文字列で、大文字と小文字が区別されます。

説明

bootfile-name コマンドは、DHCP クライアントが使用する起動ファイル名またはリモート起動ファイルの HTTP 形式の URL を設定します。

undo bootfile-name コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

起動ファイルが TFTP サーバ上にある場合は、bootfile-name パラメータを使用して、DHCP クライアントが使用する起動ファイル名を指定します。起動ファイルが HTTP サーバ上にある場合は、url パラメータを使用して、リモート起動ファイルの HTTP 形式の URL を指定します。

例

#DHCP アドレスプールの設定 0 DHCP クライアントに割り当てられる起動ファイル名は boot.cfg です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name boot.cfg

#DHCP アドレスプールの設定 0 DHCP クライアントに割り当てられた起動ファイルの HTTP URL は http://10.1.1.1/boot.cfg です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name http://10.1.1.1/boot.cfg

関連コマンド

- **display dhcp server pool**
- **next-server**
- **tftp-server domain-name**
- **tftp-server ip-address**

13.1.4 class option-group

Syntax

class *class-name* **option-group** *option-group-number*

undo class *class-name* **option-group**

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

class-name: DHCP ユーザクラスの名前を指定します。設定範囲は 1～63 文字で、大文字と小文字は区別しません。

option-group-number: DHCP オプショングループに 1 から 32768 までの番号を割り当てます。

説明

DHCP-DISCOVER メッセージを受信すると、サーバはこのコマンドで指定された順序で DHCP クライアントと DHCP ユーザクラスを比較します。一致する DHCP ユーザクラスが見つかった場合、サーバはクライアントにオプショングループの DHCP オプションを割り当てます。複数の DHCP ユーザクラスと一致した場合、サーバは次のようにオプショングループを選択します。

- オプショングループに共通のオプションがある場合、サーバは最初に一致したユーザクラスに指定されたオプショングループを選択します。
- オプショングループのオプションが異なる場合、サーバは一致するオプショングループをすべて選択します。

DHCP アドレスプール内の DHCP ユーザクラスに指定できるオプショングループは 1 つだけです。ユーザクラスに対してこのコマンドを複数回実行すると、最新の設定が有効になります。

例

DHCP アドレスプール 0 の DHCP ユーザクラス user に、DHCP オプショングループ 1 を指定します。

<Sysname> system-view

[Sysname] dhcp server ip-pool 0

[Sysname-dhcp-pool-0] class user option-group 1

関連コマンド

- **dhcp option-group**

13.1.5 dhcp class

Syntax

dhcp class *class-name*

undo dhcp class *class-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

class-name: DHCP ユーザクラスの名前を指定します。設定範囲は 1～63 文字で、大文字と小文字は区別しません。

説明

dhcp class コマンドは DHCP ユーザクラスを作成して view に移行します。あるいは、コマンドを使用して既存の DHCP ユーザクラス View に移行することができます。

undo dhcp class コマンドは指定した DHCP ユーザクラスを削除します。

DHCP ユーザクラス View では、if-match コマンドを使用して、DHCP クライアントを DHCP ユーザクラスに紐付ける一致ルールを設定できます。

例

DHCP ユーザクラス test を作成し、その View に移行します。

<Sysname> system-view

[Sysname] dhcp class test

[Sysname-dhcp-class-test]

関連コマンド

- **address range**
- **class option-group**
- **if-match**

13.1.6 dhcp option-group

Syntax

dhcp option-group *option-group-number*

undo dhcp option-group *option-group-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

option-group-number: DHCP オプショングループに 1 から 32768 までの番号を割り当てます。

説明

dhcp option-group コマンドは DHCP オプショングループを作成して view に移行します。あるいは、コマンドを使用して既存の DHCP オプショングループ View に移行することができます。

undo dhcp option-group コマンドは指定した DHCP オプショングループを削除します。

例

DHCP オプショングループ 1 を作成し、その View に移行します。

<Sysname> system-view

[Sysname] dhcp option-group 1

[Sysname-dhcp-option-group-1]

関連コマンド

- **class option-group**
- **option**

13.1.7 dhcp server apply ip-pool

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool

デフォルト

インタフェースはアドレスプールを参照しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

pool-name:DHCP アドレスプール名。1~63 文字の文字列で、大文字と小文字は区別されません。

説明

dhcp server apply ip-pool コマンドを使用して、インタフェースが参照するアドレスプールを指定します。

undo dhcp server apply ip-pool コマンドを使用して、デフォルトの状態を復元します。

このコマンドがインタフェースで設定されている場合、インタフェースは DHCP 要求を受信すると、静的にバインドされた IP アドレスをクライアントに優先的に割り当てます。静的にバインドされた IP アドレスが存在しない場合は、参照アドレスプールから IP アドレスを選択してクライアントに割り当てます。割り当て可能な IP アドレスが参照アドレスプールに存在しない場合、デバイスはクライアントに IP アドレスを割り当てることができません。

インタフェースで **dhcp server apply ip-pool** コマンドが設定されている場合、インタフェースが参照するアドレスプールが存在しないと、クライアントに IP アドレスを動的に割り当てることができません。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#設定 VLAN インタフェース 2 は DHCP アドレスプール 0 を参照します。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dhcp server apply ip-pool 0
```

関連コマンド

- **dhcp server ip-pool**

13.1.8 dhcp server forbidden-ip

Syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

undo dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

デフォルト

自動割り当てに関与しないグローバル IP アドレスが設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

start-ip-address:自動割り当てに参加していない開始 IP アドレス。

end-ip-address:自動割り当てに参加しない終了 IP アドレス。start-ip-address より小さい値は指定できません。このパラメータが指定されていない場合は、自動割り当てに参加していない IP アドレスが 1 つだけ start-ip-address になります。それ以外の場合、start-ip-address から end-ip-address までの IP アドレスは自動割り当てに参加できません。

説明

dhcp server forbidden-ip コマンドを使用して、自動割り当てに関与しないグローバル IP アドレスを設定します。

undo dhcp server forbidden-ip コマンドは、自動割り当てに関与しない IP アドレスのグローバル設定を解除するために使用します。

サーバによっては、DHCP クライアントに割り当てることができない IP アドレス(ゲートウェイアドレス、FTP サーバアドレスなど)を使用します。このコマンドを使用すると、これらのアドレスが自動割り当てに参加しなくなります。

すでに静的にバインドされている IP アドレスが、*dhcp server forbidden-ip* コマンドを使用して自動割り当てに参加しないように構成されている場合は、静的にバインドされているユーザにそのアドレスを割り当てることができます。

undo dhcp server forbidden-ip コマンドを実行して IP アドレスの自動割り当てに参加しない構成を解除する場合は、*dhcp server forbidden-ip* コマンドの実行時に指定したアドレス/アドレス範囲と一致するアドレス/アドレス範囲を指定する必要があります。自動割り当てに参加しない IP アドレスをアドレス範囲に設定した場合、そのアドレス範囲内のすべての IP アドレスを一度に構成解除できます。また、これらの IP アドレスを個別に構成解除することはできません。

dhcp server forbidden-ip コマンドを複数回実行すると、自動割り当てに関与しない複数の IP アドレスセグメントを設定できます。

例

#設定 10.110.1.1~10.110.1.63 の IP アドレスは、アドレスの自動割り当てには関与しません。

<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63

関連コマンド

- **forbidden-ip**
- **static-bind**

13.1.9 dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

デフォルト

DHCP アドレスプールがありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

pool-name:アドレスプールを一意に識別する DHCP アドレスプール名。1~63 文字の文字列で、大文字と小文字は区別されません。

説明

dhcp server ip-pool コマンドを使用して、DHCP アドレスプールを作成し、DHCP address pool view に入ります。DHCP アドレスプールがすでに作成されている場合は、DHCP address pool view に直接進みます。

undo dhcp server ip-pool コマンドを使用して、指定したアドレスプールを削除します。

DHCP アドレスプールでは、DHCP クライアントに割り当てる IP アドレス、ゲートウェイアドレスなどのパラメータを設定できます。

例

#pool1 という名前の DHCP アドレスプールを作成します。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool pool1
[Sysname-dhcp-pool-pool1]
```

関連コマンド

- **class ip-pool**
- **dhcp server apply ip-pool**
- **display dhcp server pool**

13.1.10 dhcp server ping packets

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

デフォルト

DHCP サーバが送信する ICMP エコー要求メッセージの最大数は 1 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

number:ICMP エコー要求メッセージを送信する最大数。範囲は 0~10 です。0 は、DHCP サーバが DHCP クライアントに IP アドレスを割り当てるまで、ping によってアドレスの競合が検出されないことを示します。

説明

dhcp server ping packets コマンドを使用して、DHCP サーバが送信する ICMP エコー要求メッセージの最大数を設定します。

undo dhcp server ping packets コマンドを使用して、デフォルトの状態を復元します。

IP アドレスの重複割り当てによるアドレスの競合を防ぐために、DHCP サーバはクライアントにアドレスを割り当てる前に、そのアドレスをプローブする必要があります。

DHCP サーバのアドレス検出は ping 機能によって実現されており、指定した時間内に ping 応答が得られるかどうかを検出することで、アドレス競合の有無を判断する。DHCP サーバは、宛先アドレスを割り当てる ICMP エコー要求メッセージを送信します。指定された時間内に ICMP エコー応答メッセージが受信された場合、アドレスの競合があるとみなされます。DHCP サーバは、アドレスプールから新しい IP アドレスを選択し、この操作を繰り返します。指定された時間内に ICMP エコー応答メッセージが受信されない場合、送信された ICMP エコー要求メッセージの数がこのコマンドで設定された最大数に達するまで、ICMP エコー要求メッセージの送信を続行します。ICMP エコー応答メッセージがまだ受信されていない場合は、クライアントにアドレスを割り当てて、クライアントが一意の IP アドレスを取得できるようにします。

例

#DHCP サーバが最大 10 個の ICMP エコー要求メッセージを送信するように設定します。

<Sysname> system-view
[Sysname] dhcp server ping packets 10

関連コマンド

- **dhcp server ping timeout**
- **display dhcp server conflict**
- **reset dhcp server conflict**

13.1.11 dhcp server ping timeout

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

デフォルト

DHCP サーバが ICMP エコー応答メッセージを待機するタイムアウト時間は 500 ミリ秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

milliseconds:ICMP がレスポンスメッセージをエコーするのを待つタイムアウト時間。ミリ秒単位で 0~10000 の値を指定できます。0 は、DHCP サーバが DHCP クライアントに IP アドレスを割り当てるまで、ping によってアドレスの競合が検出されないことを示します。

説明

dhcp server ping timeout コマンドを使用して、DHCP サーバが ICMP エコー応答メッセージを待機するタイムアウト時間を設定します。

undo dhcp server ping timeout コマンドを使用して、デフォルトの状態を復元します。

IP アドレスの重複割り当てによるアドレスの競合を防ぐために、DHCP サーバはクライアントにアドレスを割り当てる前に、そのアドレスをプローブする必要があります。

DHCP サーバのアドレス検出は ping 機能によって実現されており、指定した時間内に ping 応答が得られるかどうかを検出することで、アドレス競合の有無を判断する。DHCP サーバは、宛先アドレスを割り当てる ICMP エコー要求メッセージを送信します。このコマンドで指定された時間内に ICMP エコー応答メッセージが受信された場合、アドレスの競合があるとみなされます。DHCP サーバは、アドレスプールから新しい IP アドレスを選択し、この操作を繰り返します。指定された時間内に ICMP エコー応答メッセージが受信されない場合、送信されたエコー要求メッセージの数が最大になるまで、ICMP エコー要求メッセージの送信が続行されます。ICMP エコー応答メッセージがまだ受信されない場合は、クライアントにアドレスが割り当てられ、クライアントが取得した IP アドレスが一意であることが確認されます。

例

#ICMP エコー応答メッセージを待機するための DHCP サーバのタイムアウトを 1000 ミリ秒に設定します。

<Sysname> system-view
[Sysname] dhcp server ping timeout 1000

関連コマンド

- **dhcp server ping packets**
- **display dhcp server conflict**
- **reset dhcp server conflict**

13.1.12 dhcp server relay information enable

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

デフォルト

有効(Option82 を処理する)

View

System view

定義済みユーザロール

network-admin

説明

dhcp server relay information enable コマンドは DHCP サーバのオプション 82 を有効にします。

undo dhcp server relay information enable コマンドは DHCP サーバのオプション 82 を無効にします。

本コマンドが有効の場合、オプション 82 のメッセージを受信すると、DHCP サーバはオプション 82 を DHCP 応答メッセージにコピーして追加します。DHCP サーバがオプション 82 を無効するように設定されている場合、DHCP 応答メッセージにオプション 82 を追加しません。

例

DHCP サーバのオプション 82 を無効にします。
<Sysname> system-view
[Sysname] undo dhcp server relay information enable

13.1.13 display dhcp server conflict

Syntax

display dhcp server conflict [**dp-address** *ip-address* | **ip** *ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dp-address *ip-address*:指定した DP のアドレス競合情報を表示します。

ip *ip-address*:指定した IP アドレスのアドレス競合情報を表示します。

説明

display dhcp server conflict コマンドを使用して、DHCP のアドレス競合情報を表示します。

DHCP サーバは、次のような場合にアドレス競合情報を生成します。

- DHCP サーバは、クライアントに IP アドレスを割り当てる前に、ネットワーク内のホストがそのアドレスを使用していることを ping で検出します。
- DHCP クライアントは、DHCP サーバに割り当てられたアドレスの競合を報告する Decline メッセージを DHCP サーバに送信します。
- DHCP サーバは、アドレスプール内の割り当て可能なアドレスがデバイス自身のアドレスであることを検出します。

パラメータが指定されていない場合は、すべての DHCP アドレス競合情報が表示されます。

例

#すべてのアドレス競合情報を表示します。

<Sysname> display dhcp server conflict

IP addressDetect time

4.4.4.1Apr 25 16:57:20 2019

4.4.4.2Apr 25 17:00:10 2019

表 13-1 display dhcp server conflict コマンドの表示情報の説明

フィールド	説明
IP address	競合するIPアドレス
Detect time	競合が検出された時刻

関連コマンド

- **reset dhcp server conflict**

13.1.14 display dhcp server expired

Syntax

display dhcp server expired [[**dp-address** *ip-address* | **ip** *ip-address* | **mac** *mac-address*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dp-address *ip-address*:指定された DP のリース期限切れアドレスバインディング情報を表示します。

ip *ip-address*:指定した IP アドレスのリース期限切れアドレスバインディング情報を表示します。

mac *mac-address*:指定した MAC アドレスのリース期限切れバインディング情報を表示します。

pool *pool-name*:指定したアドレスプール内のリースの有効期限が切れたアドレスバインディング情報を表示します。pool-name はアドレスプール名で、大文字と小文字を区別しない 1~63 文字の文字列です。

verbose:リース期限切れアドレスバインディングの詳細を表示します。このパラメータを指定しない場合は、すべての IP アドレスのリース期限切れアドレスバインディング情報が表示されます。

説明

display dhcp server expired コマンドを使用して、リースが期限切れになったアドレスバインディング情報を表示します。

DHCP アドレスプールに使用可能なアドレスが割り当てられると、リースの期限が切れたアドレスが DHCP クライアントに割り当てられます。

パラメータが指定されていない場合は、リースが期限切れになったすべてのアドレスバインディング情報が表示されます。

例

#すべてのリースの期限切れアドレスバインディング情報を表示します。

<Sysname> display dhcp server expired

IP address Client-identifier/Hardware address Lease expiration

4.4.4.6 3030-3066-2e65-3230-302e-3130-3234 Apr 25 17:10:47 2019

-2d45-7468-6572-6e65-7430-2f31

表 13-2 display dhcp server expired コマンドの表示情報の説明

フィールド	説明
IP address	リース期限切れのIPアドレス
Client-identifier/Hardware address	リース期限切れのクライアントIDまたはMACアドレス
Lease expiration	リースの有効期限

#すべてのリースが期限切れになったアドレスの詳細なバインディング情報を表示します。

<Sysname> display dhcp server expired verbose

IP address:192.168.56.3

Pool name:1

Client-identifier:N/A

Hardware address type:Ethernet

Hardware address:0000-0000-0002

Lease expiration:Mar 16 16:00:22 2017

Remaining reservation time:136 years 2 months 6 hours 28 minutes 11 seconds

IP address reservation mode:Based on client MAC

IP address:5.5.5.5

Pool name:2

Client-identifier:0061-6161-612 e-6161-6161-2e61-6161-612d-4745-302f-302f-33

Hardware address type:Ethernet

Hardware address:0000-0000-0003

Lease expiration:Mar 16 16:00:33 2017

Remaining reservation time:136 years 2 months 6 hours 28 minutes 22 seconds

IP address reservation mode:Based on client ID

IP address:3.3.3.5

Pool name:abc

Client-identifier:0100-0000-0000-05

Hardware address type:Ethernet

Hardware address:0000-0000-0005

Lease expiration:Mar 16 16:10:33 2017

Remaining reservation time:2 months 6 hours 27 minutes 22 seconds

IP address reservation mode:Based on client MAC

表 13-3 display dhcp server expired verbose コマンドの表示情報の説明

フィールド	説明
IP address	リース期限切れのIPアドレス
Pool name	リースが存在するアドレスプール
Client-identifier	リースが期限切れのクライアントID。値N/AIは、DHCP要求メッセージにOption61情報が含まれていないことを示します。
Hardware address type	ハードウェアアドレスのタイプ。値は次のとおりです。 • Ethernet:イーサネット • Token ring:トークンリングネットワーク • Unknown:不明なグループネットワーク
Hardware address	ハードウェアアドレス
Lease expiration	リースの有効期限
Remaining reservation time	リースの保留残り時間が0の場合は、アドレスプールに古いリースが残り、削除されていることを示します。
IP address reservation mode	予約IPアドレスのタイプ。値は次のとおりです。 • Based on client ID:クライアント ID で予約 • Based on client MAC:MAC アドレスで予約

関連コマンド

- **reserve expired-ip enable**
- **reset dhcp server expired**

13.1.15 display dhcp server free-ip

Syntax

display dhcp server free-ip [**pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool *pool-name*:指定したアドレスプールの空きアドレス情報を表示します。pool-name はアドレスプール名で、大文字と小文字を区別しない 1~63 文字の文字列です。このパラメータを指定しない場合、すべてのアドレスプールの空きアドレス情報が表示されます。

説明

display dhcp server free-ip コマンドは、DHCP アドレスプールの空きアドレス情報、つまり DHCP クライアントに割り当てられていない IP アドレス情報を表示します。

例

#すべての DHCP アドレスプールの空きアドレス情報を表示します。

<Sysname> display dhcp server free-ip
Pool name: 1
  Network: 10.0.0.0 mask 255.0.0.0
    IP ranges from 10.0.0.10 to 10.0.0.100
    IP ranges from 10.0.0.105 to 10.0.0.255
  Secondary networks:
    10.1.0.0 mask 255.255.0.0
      IP ranges from 10.1.0.0 to 10.1.0.255
    10.2.0.0 mask 255.255.0.0
      IP Ranges from 10.2.0.0 to 10.2.0.255

Pool name: 2
  Network: 20.1.1.0 mask 255.255.255.0
    IP ranges from 20.1.1.0 to 20.1.1.255

表 13-4 display dhcp server free-ip コマンドの表示情報の説明

フィールド	説明
Pool name	アドレスプールの名前
Network	割り当て可能なアドレスセグメント
IP ranges	割り当て可能なアドレス範囲
Secondary networks	アドレスネットワークセグメントから割り当て可能

関連コマンド

- **address range**
- **dhcp server ip-pool**
- **network**

13.1.16 display dhcp server ip-in-use

Syntax

display dhcp server ip-in-use [[**dp-address** *ip-address* | **ip** *ip-address* | **subnet** *network-address mask-length*] [**vpn-instance** *vpn-instance-name*] | **pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dp-address *ip-address*:指定した DP のアドレスバインディング情報を表示する。

ip *ip-address*:指定した IP アドレスのアドレスバインディング情報を表示します。

subnet *network-address mask-length*:指定したサブネットセグメント内のアドレスバインディング情報を表示します。

pool *pool-name*:指定したアドレスプールのアドレスバインディング情報を表示します。pool-name はアドレスプール名で、大文字と小文字を区別しない 1~63 文字の文字列です。

パラメータを指定しない場合は、すべての IP アドレスのアドレスバインディング情報が表示されます。

説明

display dhcp server ip-in-use コマンドを使用して、DHCP アドレスバインディング情報を表示します。

DHCP サーバが DHCP クライアントのゲートウェイデバイスとして機能している場合、DHCP サーバに記録されている DHCP クライアントのアドレスバインディング情報は、他のセキュリティ機能で使用できるようになります。

注:リースの有効期限が 2100 年を超える場合は、After 2100 と表示されます。

例

#すべての DHCP アドレスバインディング情報を表示します。

<Sysname> display dhcp server ip-in-use

IP address	Client identifier/ Hardware address	Lease expiration	Type
10.1.1.1	4444-4444-4444	Not used	Static(F)
10.1.1.2	0030-3030-2e30-3030-662e-3030-3033-2d45-7468-6572-6e65-74	May 1 14:02:49 2015	Auto(C)
10.1.1.3	0133-3037-392e-3933-3037-2e39-3030-32	May 1 14:18:22 2016	Auto(C)
10.1.1.4	1111-1111-1111	After 2100	Static(C)

表 13-5 display dhcp server ip-in-use コマンドの表示情報の説明

フィールド	説明
IP address	DHCPクライアントに割り当てられたIPアドレス

フィールド	説明
Client identifier/Hardware address	クライアントIDまたはクライアントのハードウェアアドレス。クライアントIDは指定された16進文字列を使用します。通常、最初の2桁はハードウェアタイプを表します。たとえば、00はタイプなしASCII文字列を使用します。01はイーサネットです;06 トークンリングネットワーク
Lease expiration	リースの有効期限には、次の値があります。 • リースが期限切れになる特定の時間値(例:May 1 14:02:49 2015) • Not used:静的にバインドされたアドレスが特定のクライアントに割り当てられていないことを示す • Unlimited:リースが無制限であることを示します。 • After 2100:リースの有効期限が 2100 年を超えていることを示します。
Type	アドレスバインディングのタイプ。値は次のとおりです。 • Static (F) :クライアントに割り当てられていない静的バインド、つまり静的無効なバインドを示します。 • Static (O) :サーバがアドレスプールから静的にバインドされた IP アドレスを選択し、DHCP-OFFER メッセージを送信してクライアントにその IP アドレスを提供すると、そのタイプのアドレスバインド情報、つまり静的な一時バインドが生成されます。 • Static (C) :クライアントに割り当てられた静的バインディング、つまり静的公式バインディングを表します。 • Auto (O) :アドレスプールから IP アドレスを動的に選択し、その IP アドレスをクライアントに提供するための DHCP-OFFER メッセージを送信することで発生する、動的バインディングを表す一時リース. • Auto (C) :アドレスプールから IP アドレスを動的に選択し、 DHCP-ACK メッセージを送信してその IP アドレスをクライアントに割り当てることに成功したときに発生するリースを表す.

関連コマンド

- **reset dhcp server ip-in-use**

13.1.17 display dhcp server pool

Syntax

display dhcp server pool [*pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool-name:指定したアドレスプールの情報を表示します。pool-name はアドレスプール名で、大文字と小文字を区別しない 1~63 文字の文字列です。このパラメータを指定しない場合、すべてのアドレスプールの情報が表示されます。

説明

display dhcp server pool コマンドを使用して、DHCP アドレスプールの情報を表示します。

例

#すべての DHCP アドレスプールの情報を表示します。

<Sysname> display dhcp server pool
Pool name: 0
  Network 20.1.1.0 mask 255.255.255.0
  class a range 20.1.1.50 20.1.1.60
  bootfile-name abc.cfg
  dns-list 20.1.1.66 20.1.1.67 20.1.1.68
  domain-name www.aabbcc.com
  bims-server ip 192.168.0.51 sharekey cipher c3$K13OmQPi791YvQoF2Gs1E+65LOU=
  option 2 ip-address 1.1.1.1
  expired day 1 hour 2 minute 3 second 0
  reserve expired-ip enable
  reserve expired-ip mode client-id time 4294967295 limit 256000
  pool vsrp status: master

Pool name: 1
  Network 20.1.1.0 mask 255.255.255.0
  secondary networks:
    20.1.2.0 mask 255.255.255.0
    20.1.3.0 mask 255.255.255.0

```
  bims-server ip 192.168.0.51 port 50 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
  forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
  gateway-list 1.1.1.1 2.2.2.2 4.4.4.4
  nbns-list 5.5.5.5 6.6.6.6 7.7.7.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired day 1 hour 0 minute 0 second 0 allow-hint
  reserve expired-ip disable
  reserve expired-ip mode client-id time 4294967295 limit 256000
  pool vsrp status: master

Pool name: 2
  Network 20.1.1.0 mask 255.255.255.0
  address range 20.1.1.1 to 20.1.1.15
  class departmentA range 20.1.1.20 to 20.1.1.29
  class departmentB range 20.1.1.30 to 20.1.1.40
  next-server 20.1.1.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 10.1.1.2
  voice-config as-ip 10.1.1.5
  voice-config voice-vlan 3 enable
  voice-config fail-over 10.1.1.1 123*
  option 2 ip-address 1.1.1.3
  expired day 1 hour 0 minute 0 second 0
  reserve expired-ip enable
  reserve expired-ip mode mac time 100 limit 100
  pool vsrp status: master

Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
      hardware-address 00e0-00fc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
  expired unlimited
  reserve expired-ip disable
  reserve expired-ip mode client-id time 4294967295 limit 256000
  pool vsrp status: master
```

表 13-6 display dhcp server pool コマンドの表示情報の説明

フィールド	説明
Pool name	アドレスプールの名前
Network	割り当て可能なアドレスセグメント
secondary networks	アドレスネットワークセグメントから割り当て可能
address range	割り当て可能なアドレス範囲
class class-name range	指定されたDHCPユーザクラスに割り当てられたアドレス範囲
static bindings	静的にバインドされたIPアドレス、ハードウェアアドレス、またはクライアントID
option	カスタムDHCPオプション
expired	リース期間、その後の数値の単位は、日、時間、分、秒です。たとえば、expired day 1 hour 2 minute 3 second 4は、リース期間が1日2時間3分4秒であることを示します。unlimitedは、リース期間が無制限であることを示します。allow-hintは、クライアントがリース期間を決定するためのネゴシエーションを許可することを示します。
remote server	リレーアドレスプール対応するDHCPサーバアドレスこのフィールドは、DHCPリレーがリレーアドレスプールを作成してremote-serverコマンドを実行すると表示されます。
active remote server	現在アクティブなDHCPサーバアドレスこのフィールドは、DHCPリレーでリレーアドレスプールを作成し、remote-serverコマンドを実行すると表示されます。値は次のとおりです。 • all と表示されている場合は、現在構成されている DHCP サーバがすべての方法で選択されていることを示します。つまり、DHCP リレーはすべての DHCP サーバに同時に DHCP 要求メッセージを転送します。 • IP アドレスが表示されている場合は、現在構成されている DHCP サーバの選択モードがプライマリモードであり、そのアドレスが現在アクティブな DHCP サーバアドレスであることを示します。つまり、DHCP リレーは、そのアドレスに対応する DHCP サーバに DHCP 要求メッセージを転送します。
bootfile-name	DHCPクライアントに割り当てられた起動ファイル名
dns-list	DHCPクライアントに割り当てられたDNSサーバアドレス
domain-name	DHCPクライアントに割り当てられたドメイン名サフィックス
bims-server	DHCPクライアントに割り当てられたBIMSサーバ情報
forbidden-ip	DHCPアドレスプール内の自動割り当てに参加していないIPアドレス
gateway-list	DHCPクライアントに割り当てられたゲートウェイアドレス
nbns-list	DHCPクライアントに割り当てられたWINSサーバアドレス
netbios-type	DHCPクライアントに割り当てられたNetBIOSノードタイプ
next-server	DHCPクライアントに割り当てられた、次にサービスを提供するサーバのIPアドレス

フィールド	説明
tftp-server domain-name	DHCPクライアントに割り当てられたTFTPサーバ名
tftp-server ip-address	DHCPクライアントに割り当てられたTFTPサーバアドレス
voice-config ncp-ip	DHCPクライアントに割り当てられたネットワークコールプロセッサのアドレス
voice-config as-ip	DHCPクライアントに割り当てられた代替サーバのアドレス
voice-config voice-vlan	DHCPクライアントに割り当てられた音声VLAN
voice-config fail-over	DHCPクライアントに割り当てられた自動フェイルオーバーコールルーティング
reserve expired-ip enable	DHCPアドレスプールの有効化DHCPアドレスプールのエージングアドレス保持機能DHCPエージングリースを保持する機能
reserve expired-ip disable	DHCPアドレスプールのシャットダウンDHCPアドレスプールのエージングアドレス保持機能DHCPエージングリースを保持する機能
reserve expired-ip mode client-id time 4294967295 limit 256000	DHCPアドレスプールエージングアドレス予約モード、リース予約時間、およびリース予約数の上限DHCPアドレスプールは、ClientIDに従ってエージングリースを予約します。
pool vsrp status	マルチマシン・バックアップ・インスタンスにおけるデバイスのステータス。次の値をとります。 • master:本装置をマスター装置とする • backup:このデバイスはスペアデバイスとして機能します。 • down:このデバイスはマルチマシンバックアップインスタンスで実行されていません
DP_ADDR	DHCPクライアントがオンラインになっているDP CPに接続されているトンネルDPエンドアドレス
Leased	割り当てられたリースの数
Expired	エージングリースの数
Free	空きリースの数

13.1.18 display dhcp server statistics

Syntax

display dhcp server statistics [**pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool *pool-name*:指定したアドレスプールの統計情報を表示します。pool-name はアドレスプール名で、大文字と小文字を区別しない 1~63 文字の文字列です。このパラメータを指定しない場合、すべてのアドレスプールの統計情報が表示されます。

説明

display dhcp server statistics コマンドを使用して、DHCP サーバの統計情報を表示します。

例

#DHCP サーバの統計情報を表示します。

```
<Sysname> display dhcp server statistics
  Pool number:                    1
  Pool utilization:               0.39%
  Bindings:
    Automatic:                    1
    Manual:                       0
    Expired:                      0
  Conflict:                       1
  Messages received:              10
    DHCPDISCOVER:                 5
    DHCPREQUEST:                  3
    DHCPDECLINE:                  0
    DHCPRELEASE:                  2
    DHCPINFORM:                   0
    BOOTPREQUEST:                 0
  Messages sent:                  6
    DHCPOFFER:                    3
    DHCPACK:                      3
    DHCPNAK:                      0
    BOOTPREPLY:                   0
  Bad Messages:                   0
```

表 13-7 display dhcp server statistics コマンドの表示情報の説明

フィールド	説明
Pool number	指定したアドレスプールの統計を表示するときに、このフィールドが表示されないアドレスプールの数

フィールド	説明
Pool utilization	アドレスプールの使用率 • すべての DHCP リース統計を表示すると、すべてのアドレスプールの全体的な使用率が表示されます。 • 指定されたアドレスプールのリース統計が表示された場合、そのアドレスプールの使用率
Bindings	アドレスバインディングの数は、次のとおりです。 • Automatic:動的に割り当てられた IP アドレスバインディングの数 • Manual:手動でバインドされた IP アドレスのバインド数 • Expired:リースが期限切れになった IP アドレスバインディングの数
Conflict	指定されたアドレスプールの統計を表示するときに、このフィールドがない競合アドレスの合計数
Messages received	DHCPサーバがDHCPクライアントから送信されたメッセージを受信した数。 • DHCPDISCOVER • DHCPREQUEST • DHCPDECLINE • DHCPRELEASE • DHCPINFORM • BOOTPREQUEST 指定されたアドレスプールの統計情報を表示するフィールドがありません
Messages sent	DHCPサーバがDHCPクライアントに送信するメッセージの数。 • DHCPOFFER • DHCPACK • DHCPNAK • BOOTPREPLY 指定されたアドレスプールの統計情報を表示するフィールドがありません
Bad Messages	指定されたアドレスプールの統計情報を表示するフィールドがない場合のエラー数

関連コマンド

- **reset dhcp server statistics**

13.1.19 dns-list

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

デフォルト

DHCP アドレスプールが構成されていない DHCP クライアントに割り当てられた DNS サーバアドレス。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>:DNS サーバの IP アドレス。&<1-8>は、最大 8 個の IP アドレスをスペースで区切って入力できることを意味します。

説明

dns-list コマンドを使用して、DHCP アドレスプールが DHCP クライアントに割り当てる DNS サーバアドレスを設定します。

undo dns-list コマンドを使用して、DHCP アドレスプールによって DHCP クライアントに割り当てられた DNS サーバアドレスを削除します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

undo dns-list コマンドの実行時にパラメータを指定しないと、DHCP アドレスプール内のすべての DNS サーバアドレスが削除されます。

例

#DHCP アドレスプールの設定 0 DHCP クライアントに割り当てられる DNS サーバアドレスは 10.1.1.254 です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254

関連コマンド

- **display dhcp server pool**

13.1.20 domain-name

Syntax

domain-name *domain-name*

undo domain-name

デフォルト

DHCP アドレスプールが構成されていない DHCP クライアントに割り当てられたドメイン名。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

domain-name:DHCP クライアントのドメイン名。1~50 文字の文字列で、大文字と小文字が区別されます。

説明

domain-name コマンドを使用して、DHCP アドレスプールが DHCP クライアントに割り当てるドメイン名を設定します。

undo domain-name コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#DHCP アドレスプールの設定 0 DHCP クライアントに割り当てられたドメイン名は company.com です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name company.com

関連コマンド

- **display dhcp server pool**

13.1.21 expired

Syntax

expired { **allow-hint** | { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** } [**allow-hint**] }

undo expired

デフォルト

DHCP アドレスプール内の IP アドレスのリース有効期間は 1 日です。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

allow-hint： DHCP クライアントが DHCP サーバと交渉してリースの有効期間(アドレスプールに設定されているリース期間とクライアントが期待するリース期間のうち、小さい方の値を取得します。)を決定できることを示します。このパラメータが指定されていない場合、アドレスプールに設定されているリース期間に基づいて、クライアントの予想されるリース期間は無視されます。

day *day*:リースが期限切れになる日数を指定します。day は 0~365 の範囲で指定します。

hour *hour*:リースが期限切れになる時間数を 0~23 時間の範囲で指定します。このパラメータが指定されていない場合、指定された有効期限の時間は 0 です。

minute *minute*:リースが期限切れになる分数を指定します。minute は 0~59 の範囲の値を取ります。このパラメータが指定されていない場合、指定された有効期限の分数は 0 です。

second *second*:リースが期限切れになる秒数を指定します。second は 0~59 の範囲の値を取ります。このパラメータが指定されていない場合、指定された有効期限の秒数は 0 です。

unlimited:有効期間は無制限です(実際のシステムは約 136 年に限定されています)。

説明

expired コマンドは、DHCP アドレスプールに割り当てられた IP アドレスのリース有効期間を設定します。

undo expired コマンドを使用して、デフォルトの状態を復元します。

DHCP サーバは、DHCP アドレスプールから IP アドレスを選択して DHCP クライアントに割り当てると、そのアドレスプールの IP アドレスのリース有効期限も DHCP クライアントに通知します。リースの有効期限が切れる前に、DHCP クライアントは更新申請を行う必要があります。更新に成功すると、DHCP クライアントはその IP アドレスを引き続き使用できます。そうしないと、リースの有効期間が経過すると、DHCP クライアントはその IP アドレスを使用できなくなり、DHCP サーバはそのアドレスを期限切れのリース情報に追加します。

例

#設定アドレスプール 0 の IP アドレスリースは、2 時間 3 分 4 秒間有効です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4

#アドレスプール 0 の IP アドレスリース有効期間を 1 日 2 時間 3 分 4 秒に設定し、DHCP クライアントが DHCP サーバと交渉してリース有効期間を決定できるようにします。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4 allow-hint

関連コマンド

- **display dhcp server expired**
- **display dhcp server pool**
- **reset dhcp server expired**

13.1.22 forbidden-ip

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip [*ip-address*&<1-8>]

デフォルト

自動割り当てに参加していないアドレスプールの IP アドレスが設定されていません。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>:アドレスプール内の自動割り当てに参加していない IP アドレス。&<1-8>は、最大 8 個の IP アドレスをスペースで区切って入力できることを意味します。

説明

forbidden-ip コマンドは、自動割り当てに参加しない IP アドレスをアドレスプールに設定します。

undo forbidden-ip コマンドは、自動割り当てに参加していない IP アドレスをアドレスプールから削除するために使用します。

DHCP address pool view で **forbidden-ip** コマンドを使用して自動割り当てに参加しない IP アドレスを設定すると、現在のアドレスプールだけが IP アドレスを割り当てることができず、他のアドレスプールも IP アドレスを割り当てることができます。

forbidden-ip コマンドを複数回実行すると、自動割り当てに関与しない複数の IP アドレスを設定できます。アドレスプールあたり最大 4096 個のアドレスを設定できます。

undo forbidden-ip コマンドの実行時にパラメータが指定されていない場合は、自動割り当てに関与しないすべての IP アドレスが削除されます。

例

#自動割り当てに参加しない DHCP アドレスプール 0 の IP アドレスを 192.168.1.3 および 192.168.1.10 に設定します。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10

関連コマンド

- **dhcp server forbidden-ip**
- **display dhcp server pool**

13.1.23 gateway-list

Syntax

gateway-list *ip-address*&<1-64> [**export-route**]

undo gateway-list [*ip-address*&<1-64>] [**export-route**]

デフォルト

DHCP アドレスプール、DHCP スレーブは、DHCP クライアントに割り当てられたゲートウェイアドレスで構成されていません。

View

DHCP address pool view

DHCP secondary subnet view

定義済みユーザロール

network-admin

パラメータ

ip-address& <1-64>:ゲートウェイの IP アドレス。&<1-64>は、最大 64 個の IP アドレスをスペースで区切って入力できることを意味します。ゲートウェイアドレスは DHCP クライアントと同じネットワークセグメントにある必要があります。

export-route:ゲートウェイリストの情報をアドレス管理に送り、クライアントからの ARP 要求に応答することで、異なる種類のトラヒックを誘導することができる。このパラメータが指定されていない場合、ゲートウェイリスト情報はアドレス管理に送信されません。

説明

gateway-list コマンドは、DHCP サーバが DHCP クライアントに割り当てるゲートウェイアドレスを設定します。

undo gateway-list コマンドは、DHCP サーバが DHCP クライアントに割り当てたゲートウェイアドレスを削除するために使用します。

DHCP サーバは、次の方法でセカンダリサブネット上のクライアントにゲートウェイアドレスを割り当てます。

- DHCP address pool view と DHCP secondary subnet view の両方でゲートウェイが指定されている場合、DHCP は DHCP secondary subnet view で指定されたものを割り当てます。
- ゲートウェイが DHCP address pool view で指定されていて、DHCP secondary subnet view で指定されていない場合、DHCP は DHCP address pool view で指定されたものを割り当てます。

パラメータを指定しない場合、undo gateway-list コマンドはすべてのゲートウェイアドレスを削除します。

例

#DHCP アドレスプールの設定 0 DHCP クライアントに割り当てられたゲートウェイアドレスは 10.1.1.1 です。

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.1.1.1
```

関連コマンド

- **display dhcp server pool**

13.1.24 if-match

Syntax

if-match rule *rule-number* **{ hardware-address** *hardware-address* **mask** *hardware-address-mask* **| option** *option-code* **[ascii** *ascii-string* **[offset** *offset* **| partial] | hex** *hex-string* **[mask** *mask* **| offset** *offset* **length** *length* **| partial]] | relay-agent** *gateway-address* **}**

undo if-match rule *rule-number*

デフォルト

設定なし

View

DHCP user class view

定義済みユーザロール

network-admin

パラメータ

rule *rule-number*: ルールに割り当てる ID を指定します。値の範囲は 1～128 までで、ID が小さいほど、一致の優先度が高くなります。

hardware-address *hardware-address*: ハードウェアアドレスをハイフンで区切られた 16 進数の文字列で指定します。値の範囲は 4～39 文字です。最後の 16 進数は 2 桁または 4 桁で、その他の 16 進数は 4 桁である必要があります。たとえば、aabb-ccdd-ee は有効で、aabb-c-dddd または aabb-cc-dddd は無効です。

mask *hardware-address-mask*: hardware-address と AND 演算するマスクを指定します。マスクの長さはハードウェアアドレスと同じである必要があります。

option *option-code*: DHCP オプションの番号を指定します。1～254 の数値で指定します。

ascii *ascii-string*: ASCII 文字列を指定します。1～128 文字の文字列で指定します。

offset *offset*: 一致操作が開始されるまでのオフセットをバイト単位で指定します。値の範囲は 0～254 です。オフセット値を指定しない場合は、オプション内容の先頭バイトから照合が開始されます。ASCII 文字列を指定した場合、オフセット後のオプションの内容が ASCII 文字列と同じであれば、パケットはルールに一致します。16 進数を指定した場合、オフセット後の指定した長さのオプション内容が 16 進数と同じであれば、パケットはルールに一致します。

partial: 部分一致を有効にします。パケット内の指定されたオプションに、ルールで指定された ASCII 文字列または 16 進数が含まれている場合、パケットはルールに一致します。たとえば、ルールで abc を指定した場合、オプションの内容 xabc、xyzabca、xabcyz、および abcxyz はすべてルールに一致します。

hex *hex-string*: 16 進数の文字列を指定します。16 進数の文字列の長さは 2～256 までの偶数である必要があります。

mask *mask*: 一致操作の 16 進数マスクを指定します。マスク長は 2～256 までの偶数で、hex-string の文字列長と同じである必要があります。DHCP サーバは、マスク長のオプション内容を先頭から選択し、選択したオプション内容と指定した 16 進数をマスクと AND 演算します。2 つの AND 演算結果が同じ場合、パケットはルールと一致します。

length *length*: 照合するオプション内容の長さをバイト単位で指定します。値の範囲は 1～128 です。長さは、*hex-string* の長さと同じである必要があります。

relay-agent *gateway-address*: giaddr フィールドの値を指定します。値はドット付き 10 進表記の IPv 4 アドレスです。パケットの giaddr フィールド値がルールの値と同じ場合、パケットはルールに一致します。

説明

if-match コマンドは DHCP ユーザクラスの一致ルールを設定します。

undo if-match コマンドは DHCP ユーザクラスの一致ルールを削除します。

DHCP クライアントによって送信された DHCP 要求が DHCP ユーザクラスのルールと一致する場合、DHCP クライアントはユーザクラスと一致します。

DHCP ユーザクラスに複数の一致ルールを設定できます。各一致ルールは、そのタイプ(ハードウェアアドレス、オプション、またはリレーエージェントアドレス)内のルール ID によって一意に識別されます。

- 設定するルールの ID とタイプが既存のルールと同じ場合、新しいルールによって既存のルールが上書きされます。
- 設定するルールの ID が既存のルールと同じでタイプが異なる場合、新しいルールが有効になり、既存のルールと共存します。ベストプラクティスとして、異なるタイプのルールに同じ ID を割り当てないでください。
- 異なる ID のルールに同じルールコンテンツを設定することはできません。

if-match hardware-address ルールを設定する場合は、次の注意事項に従ってください。

- ハードウェアアドレスタイプは MAC アドレスだけをサポートします。ルールは、他のタイプのハードウェアアドレスを持つクライアントと一致しません。
- 指定するハードウェアアドレスは、一致するクライアントハードウェアアドレスと同じ長さである必要があります。MAC アドレスを一致させるには、指定するハードウェアアドレスの長さが 6 バイトである必要があります。
- ハードウェア一致操作のマスク内の fs と 0 は連続していなくてもかまいません。たとえば、if-match rule 1 hardware-address 0094-0000-1100 mask ffff-0000-ff00 のルールでは、最初の 2 バイトが 0094、5 番目のバイトが 11 であるハードウェアアドレスと一致します。

if-match option ルールを設定するときは、次の注意事項に従ってください。

- オプションを含むパケットを照合するには、option-code 引数だけを指定します。
- AND 演算で 16 進数を照合するには、option option-code hex hex-string mask mask プションを指定します。
- 16 進数を直接照合するには、option option-code hex hex-string [offset offset length length | partial]オプションを指定します。offset、length、または partial パラメータを指定しない場合、オプションの内容が 16 進数で始まると、パケットはルールに一致します。
- ASCII 文字列と一致させるには、option option-code ascii ascii-string [offset offset | partial]オプションを指定します。offset または partial パラメータを指定しない場合、オプションの内容が ASCII 文字列で始まると、パケットはルールと一致します。

例

ハードウェアアドレスが 6 バイト長で 0094 で始まる DHCP 要求と一致するように、DHCP ユーザクラス exam の一致ルール 1 を設定します。

<Sysname> system-view

[Sysname] dhcp class exam

[Sysname-dhcp-class-exam] if-match rule 1 hardware-address 0094-0000-0101 mask ffff-0000-0000

関連コマンド

- **dhcp class**

13.1.25 nbns-list

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list [*ip-address*&<1-8>]

デフォルト

DHCP アドレスプールが構成されていない DHCP クライアントに割り当てられた WINS サーバアドレス。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address& <1-8>:WINS サーバの IP アドレス。&<1-8>は、最大 8 個の IP アドレスをスペースで区切って入力できることを意味します。

説明

nbns-list コマンドを使用して、DHCP アドレスプールが DHCP クライアントに割り当てる WINS サーバアドレスを設定します。

undo nbns-list コマンドを使用して、DHCP アドレスプールが DHCP クライアントに割り当てた WINS サーバアドレスを削除します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

undo nbns-list コマンドの実行時にパラメータが指定されていない場合は、DHCP アドレスプール内のすべての WINS サーバアドレスが削除されます。

例

#DHCP アドレスプールの設定 0 DHCP クライアントに WINS サーバアドレス 10.1.1.1 を割り当てます。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.1.1.1

関連コマンド

- **display dhcp server pool**
- **netbios-type**

13.1.26 netbios-type

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

デフォルト

DHCP アドレスプールが構成されていない DHCP クライアントに割り当てられた NetBIOS ノードタイプ。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

b-node:クラス b ノード。 「b」 はブロードキャスト(broadcast)を表し、ホスト名と IP アドレス間のマッピングをブロードキャストで取得します。送信元ノードは、宛先ノードのホスト名を持つブロードキャストメッセージを送信することで宛先ノードの IP アドレスを取得し、宛先ノードはブロードキャストメッセージを受信すると、自分の IP アドレスを送信元ノードに返す。

h-node:h クラスノード 「h」 はハイブリッド(hybrid)を表し、 「エンドツーエンド」通信機構を持つ b クラスノードである。このようなノードは、まずユニキャストメッセージを送信して WINS サーバと通信してマッピング関係を取得し、取得できなければブロードキャストメッセージを送信してマッピング関係を取得する。

m-node:m クラスノード 「m」 は混合(mixed)を表し、部分ブロードキャスト特性を持つ p クラスノードです。このようなノードは、まずブロードキャストメッセージを送信してマッピング関係を獲得し、獲得できなければユニキャストメッセージを送信して WINS サーバと通信し、マッピング関係を獲得する。

p-node:クラス p ノード。「p」 はエンドツーエンド(peer-to-peer)を表します。つまり、このクラスのノードは、ユニキャストメッセージを送信して WINS サーバと通信することでマッピング関係を取得します。ソースノードは WINS サーバにユニキャストメッセージを送信し、 WINS サーバはユニキャストメッセージを受信すると、ソースノードが要求した宛先ノード名に対応する IP アドレスを返す。

説明

netbios-type コマンドを使用して、DHCP アドレスプールが DHCP クライアントに割り当てる NetBIOS ノードタイプを設定します。

undo netbios-type コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#DHCP アドレスプールの設定 0 DHCP クライアントに割り当てられた NetBIOS ノードタイプはクラス p ノードです。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type p-node

関連コマンド

- **display dhcp server pool**
- **nbns-list**

13.1.27 network

Syntax

network *network-address* [*mask-length* | **mask** *mask*] [**export-route** [**preference** *preference* | **tag** *tag*] *] [**secondary**]

undo network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

デフォルト

動的に割り当てられる IP アドレスが構成されていないネットワークセグメント。割り当て可能な IP アドレスがありません。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

network-address:動的に割り当てるセグメントアドレス。マスク長とマスクが指定されていない場合は、自然なマスクが使用されます。

mask-length:IP アドレスのネットマスク長。範囲は 1~30 です。

mask *mask*:IP アドレスのネットマスク。mask は 10 進数です。

export-route:指定されたセグメント情報を発行するルート管理にセグメント情報を送信します。指定されたネットワークセグメントのダウンストリームトラフィックをブートします。このパラメータを指定しない場合、セグメント情報はルーティング管理に送信されません。

preference *preference*:ルート管理ネットワークセグメントに送信されるルートのプライオリティ。preference の範囲は 1~255 で、デフォルト値は 70 です。

tag *tag*:ルート管理のセグメントルートに送信されるタグ値。tag の範囲は 0~4294967295 で、デフォルト値は 0 です。tag フィールドは、ルーティングポリシーが tag フィールドに基づいてルーティングエントリをフィルタリングできるネットワークセグメントのルートを識別します。

secondary:設定されたネットワークセグメントをスレーブセグメントとして指定します。このパラメータが指定されていない場合は、構成されているネットワークセグメントがプライマリセグメントであることを示します。プライマリセグメントにアドレスが割り当てられると、DHCP サーバは、ネットワークセグメントから DHCP クライアントに割り当てるアドレスを選択できます。

説明

DHCP アドレスプールによって動的に割り当てられる IP アドレスのセグメントを設定するには、**network** コマンドを使用します。

undo network コマンドを使用して、動的割り当て用に作成された IP アドレスセグメントを削除します。

secondary キーワードを使用すると、セカンダリサブネットを指定してその view を入力できます。DHCP secondary subnet view では、セカンダリサブネットの DHCP クライアントに対して **gateway-list** コマンドを使用して、ゲートウェイを指定できます。

DHCP アドレスプールに指定できるプライマリサブネットは 1 つだけです。**network** コマンドを複数回実行すると、最新の設定が有効になります。

DHCP アドレスプールには、最大 32 のセカンダリサブネットを指定できます。

DHCP アドレスプール内のプライマリサブネットとセカンダリサブネットは、同じネットワークアドレスとマスクを持つことはできません。

アドレスプールで **address range** または **class** コマンドを使用した場合、同じアドレスプール内にセカンダリサブネットを指定することはできません。

ネットワーク設定を変更または削除すると、現在のアドレスプールから割り当てられたアドレスが削除されます。

network export-route コマンドを複数回実行すると、最新の設定が有効になります。

例

#DHCP アドレスプールの設定 0 動的に割り当てられるプライマリアドレスセグメントは 192.168.8.0/24 で、セカンダリアドレスセグメントは 192.168.10.0/24 です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
[Sysname-dhcp-pool-0] network 192.168.10.0 mask 255.255.255.0 secondary
[Sysname-dhcp-pool-0-secondary]

関連コマンド

- **display dhcp server pool**
- **gateway-list**
- **subnet alloc-mode**
- **subnet export-route disable**
- **subnet idle-time**
- **subnet mask-length**

13.1.28 next-server

Syntax

next-server *ip-address*

undo next-server

デフォルト

DHCP アドレスプールが構成されていない DHCP クライアントに次にサービスを提供するサーバの IP アドレスが割り当てられています。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address:次にサービスを提供するサーバの IP アドレス。

説明

next-server コマンドは、DHCP クライアントに次にサービスを提供するサーバ IP アドレスを割り当てるために、DHCP アドレスプールを設定します。

undo next-server コマンドを使用して、デフォルトの状態を復元します。

DHCP クライアントに次にサービスを提供するサーバの IP アドレスは、 DHCP クライアントの起動時に IP アドレスを取得した後、別の起動データを取得するためのサーバアドレスである。たとえば、TFTP サーバアドレス。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#DHCP アドレスプールの設定 0 DHCP クライアントが次にサービスを提供するサーバに割り当てる IP アドレスは 10.1.1.254 です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] next-server 10.1.1.254

関連コマンド

- **display dhcp server pool**

13.1.29 option

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

undo option *code*

デフォルト

DHCP オプションがカスタマイズされていません。

View

DHCP address pool view

DHCP option group view

定義済みユーザロール

network-admin

パラメータ

code:50~54、56、58、59、61、82 を除く 2~254 の値を持つオプションの数値。

ascii *ascii-string*:オプションの内容が設定されている ASCII 文字列を指定します。ascii-string は 1~255 文字の ASCII 文字列で、大文字と小文字が区別されます。

hex *hex-string*:オプションの内容が設定されている 16 進数を指定します。hex-string は 16 進数で、桁数の範囲は 2~256 の偶数です。

ip-address *ip-address*& <1-8>:オプションがに設定されている IP アドレスを指定します。&<1-8>は、最大 8 個の IP アドレスをスペースで区切って入力できることを意味します。

説明

option コマンドを使用して、DHCP オプションをカスタマイズします。

undo option コマンドを使用して、カスタム DHCP オプションを削除します。

このコマンドを実行すると､DHCP 応答メッセージ内の code という番号のオプションを、指定した ASCII 文字列、16 進数、または IP アドレスに設定して、クライアントに割り当てることができます。

このコマンドを使用すると、DHCP サーバに柔軟なオプション構成が提供されるため、DHCP サーバは DHCP クライアントにより豊富なオプションを提供できます。このコマンドを使用すると、次の場合に DHCP オプションをカスタマイズできます。

- DHCP の進化に伴い、新しい DHCP オプションが次々と登場しています。DHCP オプションをカスタマイズすると、新しい DHCP オプションを簡単に追加できます。
- 一部のオプションの内容は、RFC では統一されていません。ベンダーは、Option 43 などのオプションの内容を必要に応じて定義できます。カスタム DHCP オプションを使用すると、ベンダー指定の情報を DHCP クライアントに提供できます。
- デバイスで使用できるオプション設定コマンドは限られていますが(例:gateway-list、dns-list コマンド)、特別なコマンドを使用せずに DHCP オプションを設定する場合は、option コマンドを使用してオプションを設定できます。たとえば、DHCP クライアントに割り当てるタイムサーバアドレスを 1.1.1.1 にするには、option 4 ip-address 1.1.1.1 コマンドを使用します。
- 既存の DHCP オプションを拡張します。現在提供されている方法ではユーザのニーズを満たすことができない場合(例えば、dns-list コマンドでは最大 8 つの DNS サーバアドレスしか設定できません｡ユーザが 8 より多くの DNS サーバアドレスを設定する必要がある場合、このコマンドでは要件を満たすことができません。)、DHCP オプションをカスタマイズすることで拡張できます。

一部の DHCP オプションは、特殊なコマンドまたは option コマンドを使用して構成できます。たとえば、Option 6 (DNS サーバー・アドレス・オプション)は、dns-list コマンドと option 6 コマンドの両方で設定できます。これらのオプションが両方とも設定されている場合は、DHCP 応答メッセージのオプションを設定するときに、特殊なコマンドの設定が優先されます。特殊なコマンドを使用して構成されていない場合は、option コマンドで構成されているコンテンツの入力オプションが使用されます。

DHCP オプショングループのオプション番号と DHCP アドレスプールのオプション番号が同じで、ユーザクラスに一致する場合、DHCP サーバは DHCP クライアントメッセージに応答して、DHCP オプショングループのオプション番号を使用します。

DHCP サーバがクライアントメッセージを応答する際に、複数の DHCP オプショングループのオプション番号が同じ場合は、最初に一致した DHCP ユーザクラスに対応する DHCP オプショングループのオプションを優先する。

このコマンドを複数回実行し、同じオプション数値 code を指定すると、最後に実行したコマンドが有効になります。

例

#Log Server オプションの番号は 7 です。DHCP クライアントに割り当てられた DHCP アドレスプール 0 のログサーバアドレスは 2.2.2.2 です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 7 ip-address 2.2.2.2

関連コマンド

- **display dhcp server pool**

13.1.30 reset dhcp server conflict

Syntax

reset dhcp server conflict [**ip** *ip-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*:指定した IP アドレスの競合情報をクリアします。このパラメータが指定されていない場合は、すべてのアドレスの競合情報がクリアされます。

説明

reset dhcp server conflict コマンドは、DHCP のアドレス競合情報をクリアするために使用します。

アドレスの競合は、一般的に、ネットワーク構成が不適切であるため、動的に割り当てられたアドレスと、ネットワーク内で静的に構成されたアドレスが競合することによって発生します。ネットワーク構成を適切に調整して競合がなくなった場合は、元の競合アドレスが競合しなくなり、再割り当てが可能になります。このとき、本コマンドにより、検出された衝突アドレスをクリアすれば、そのアドレスを再割当てすることができる。

例

#すべてのアドレス競合情報をクリアします。

<Sysname> reset dhcp server conflict

関連コマンド

- **display dhcp server conflict**

13.1.31 reset dhcp server expired

Syntax

reset dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*:指定した IP アドレスのリース期限切れアドレスバインディング情報をクリアします。このパラメータを指定しない場合は、すべての IP アドレスのリース期限切れアドレスバインディング情報がクリアされます。

pool *pool-name*:指定されたアドレスプールからリースが期限切れになったアドレスバインディング情報をクリアします。pool-name はアドレスプール名で、大文字と小文字を区別しない 1~63 文字の文字列です。このパラメータが指定されていない場合は、すべてのアドレスプールのリース期限切れアドレスバインディング情報がクリアされます。

説明

reset dhcp server expired コマンドは、リースが期限切れになったアドレスバインディング情報をクリアするために使用します。

例

#すべてのリースが期限切れになったアドレスバインディング情報をクリアします。

<Sysname> reset dhcp server expired

関連コマンド

- **display dhcp server expired**

13.1.32 reset dhcp server ip-in-use

Syntax

reset dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*:指定した IP アドレスの正式バインディングおよび一時バインディング情報をクリアします。このパラメータが指定されていない場合は、すべての IP アドレスの正式および一時バインド情報がクリアされます。

pool *pool-name*:指定されたアドレスプールの正式バインディングおよび一時バインディング情報をクリアします。pool-name はアドレスプール名で、大文字と小文字を区別しない 1~63 文字の文字列です。このパラメータが指定されていない場合は、すべてのアドレスプールの正式および一時バインド情報がクリアされます。

説明

reset dhcp server ip-in-use コマンドを使用して、DHCP の正式バインディングおよび一時バインディング情報をクリアします。

静的正式バインディング情報を消去すると、静的無効バインディングになります。

例

#アドレス 10.110.1.1 の正式バインディングおよび一時バインディング情報をクリアします。

<Sysname> reset dhcp server ip-in-use ip 10.110.1.1

関連コマンド

- **display dhcp server ip-in-use**

13.1.33 reset dhcp server statistics

Syntax

reset dhcp server statistics

View

User view

定義済みユーザロール

network-admin

説明

reset dhcp server statistics コマンドは、DHCP サーバの統計情報をクリアするために使用します。

例

#DHCP サーバの統計情報をクリアします。

<Sysname> reset dhcp server statistics

関連コマンド

- **display dhcp server statistics**

13.1.34 snmp-agent trap enable dhcp server

Syntax

snmp-agent trap enable dhcp server [**address-exhaust** | **allocated-ip** | **ip-in-use**]

undo snmp-agent trap enable dhcp server

デフォルト

DHCP サーバのアラーム機能はすべてオンになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

address-exhaust:単一の DHCP アドレスプールのアドレスリソースが枯渇/回復したことを示すアラーム情報。

allocated-ip:DHCP サーバ上のすべてのアドレスプールのアドレス割り当て成功率が過去 5 分間にしきい値を下回ったことを示すアラーム情報。しきい値を設定するには、dhcp server allocated-ip threshold コマンドを使用します。

ip-in-use:単一の DHCP アドレスプールの使用率がサンプリング時点でしきい値を超えていることを示すアラーム情報。しきい値を設定するには、ip-in-use threshold コマンドを使用します。

説明

snmp-agent trap enable dhcp server コマンドを使用して、DHCP サーバのアラーム機能をオンにします。

undo snmp-agent trap enable dhcp server コマンドを使用して、DHCP サーバのアラーム機能をオフにします。

パラメータが指定されていない場合、DHCP サーバのすべてのタイプのアラーム機能が有効になります。

DHCP サーバーモジュールのアラーム機能を有効にすると、モジュールの重要なイベントを報告するアラーム情報が生成されます。生成されたアラーム情報はデバイスの SNMP モジュールに送信され、SNMP 内のアラーム情報の送信パラメータを設定することにより、アラーム情報の出力に関する属性が決定されます。

アラーム情報の送信設定の詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

例

#DHCP サーバのすべてのアラーム機能をオンにします。

<Sysname> system-view
[Sysname] snmp-agent trap enable dhcp server

#DHCP サーバアドレスプールのアドレスリソース枯渇/回復のアラーム機能を有効にします。

<Sysname> system-view
[Sysname] snmp-agent trap enable dhcp server address-exhaust

#DHCP サーバのアドレス割り当て成功率がしきい値アラーム機能を下回っています。

<Sysname> system-view
[Sysname] snmp-agent trap enable dhcp server allocated-ip

#DHCP サーバアドレスプールの使用率がしきい値を超えた場合にアラームを有効にします。

<Sysname> system-view
[Sysname] snmp-agent trap enable dhcp server ip-in-use

関連コマンド

- dhcp server allocated-ip threshold
- ip-in-use threshold
- snmp-agent target-host（ネットワーク管理および監視コマンドリファレンス/SNMP)

13.1.35 static-bind

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] }

undo static-bind ip-address *ip-address*

デフォルト

DHCP アドレスプールに静的アドレスバインディングが設定されていません。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address *ip-address*:静的バインドの IP アドレスを指定します。マスク長とマスクが指定されていない場合は、自然なマスクが使用されます。

mask-length:静的にバインドされた IP アドレスのマスク長、つまりマスク内の連続する「1」 の数。範囲は 1~30 です。

mask *mask*:静的にバインドされた IP アドレスのマスクを指定します。マスクは 10 進ドット表記です。

client-identifier *client-identifier*:静的バインドのクライアント ID を指定します。client-identifier は、クライアント ID を表す 4~254 文字の文字列で、16 進数と 「-」 のみを含む H-H-H ...形式の文字列です。最後の H は 2 桁または 4 桁の 16 進数を表し、それ以外は 4 桁の 16 進数を表します。たとえば、aabb-cccc-dd は有効な ID、aabb-c-dddd と aabb-cc-dddd は無効なクライアント ID です。

hardware-address *hardware-address*:静的にバインドされたクライアントのハードウェアアドレスを指定します。hardware-address は、クライアントのハードウェアアドレスを示す 4~39 文字の文字列で、16 進数と 「-」 のみを含む H-H-H ...形式です。最後の H は 2 桁または 4 桁の 16 進数以外は 4 桁の 16 進数です。たとえば、aabb-cccc-dd は有効なクライアントハードウェアアドレスで、aabb-c-dddd と aabb-cc-dddd は無効なクライアントハードウェアアドレスです。

ethernet:クライアントのハードウェアアドレスのタイプが Ethernet で、デフォルトが Ethernet であることを指定します。

token-ring:クライアントのハードウェアアドレスタイプをトークンリングネットワークに指定します。

説明

static-bind コマンドを使用すると、DHCP アドレスプールで静的アドレスバインディングを設定して、クライアント ID またはハードウェアアドレスが指定されたクライアントに DHCP サーバが固定 IP アドレスを割り当てることができます。

undo static-bind コマンドは、DHCP アドレスプールから静的アドレスバインディングを削除するために使用します。

静的にバインドされた IP アドレスを DHCP サーバのインタフェース IP アドレスにすることはできません。そうしないと、IP アドレスの競合が発生し、バインドされたクライアントは IP アドレスを正しく取得できなくなります。

同じアドレスプールに複数の静的アドレスバインディングを設定できます。すべてのアドレスプールに設定された静的アドレスバインディングは、合計で 8192 を超えることはできません。

同じアドレスは 1 つのクライアントにのみバインドできます。このコマンドを繰り返し実行しても、IP アドレスとクライアントのバインディング関係を変更することはできません。IP アドレスとクライアントのバインディング関係を変更するには、**undo static-bind** コマンドを使用して静的アドレスバインディングを削除してから、**static-bind** コマンドを実行します。

例

#DHCP アドレスプール 0 の設定:クライアント ID が 00 aa-aabb のクライアントに、IP アドレス 10.1.1.1/24 を固定的に割り当てます。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0 client-identifier 00aa-aabb

関連コマンド

- **display dhcp server pool**

13.1.36 tftp-server domain-name

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

デフォルト

DHCP アドレスプールが DHCP クライアントに割り当てられている TFTP サーバドメイン名が設定されていません。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

domain-name:TFTP サーバのドメイン名。1~63 文字の文字列で、大文字と小文字が区別されます。

説明

tftp-server domain-name コマンドを使用して、DHCP アドレスプールが DHCP クライアントに割り当てる TFTP サーバドメイン名を設定します。

undo tftp-server domain-name コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#DHCP アドレスプールの設定 0 DHCP クライアントに割り当てられる TFTP サーバのドメイン名は aaa です。

<Sysname> system-view

[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa

関連コマンド

- **display dhcp server pool**
- **tftp-server ip-address**

13.1.37 tftp-server ip-address

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

デフォルト

DHCP アドレスプールが設定されていません DHCP クライアントに割り当てられた TFTP サーバアドレス。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address:TFTP サーバの IP アドレス。

説明

tftp-server ip-address コマンドを使用して、DHCP アドレスプールが DHCP クライアントに割り当てる TFTP サーバアドレスを設定します。**undo tftp-server ip-address** コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#DHCP アドレスプールの設定 0 DHCP クライアントに 10.1.1.1 の TFTP サーバアドレスを割り当てます。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1

関連コマンド

- **display dhcp server pool**
- **tftp-server domain-name**

13.1.38 voice-config

Syntax

voice-config { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

デフォルト

DHCP アドレスプールが構成されていない DHCP クライアントに割り当てられた Option 184 コンテンツ。

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

as-ip *ip-address*:スタンバイサーバの IP アドレスを指定します。

fail-over *ip-address dialer-string*:自動フェイルオーバーIP アドレスとコール文字列を指定します。dialer-string は 1~39 文字の文字列で、数字の 0~9 と 「*」 のみを使用できます。

ncp-ip *ip-address*:ネットワークコールプロセッサの IP アドレスを指定します。

voice-vlan *vlan-id*:音声 VLAN の ID を指定します。vlan-id 値の範囲は 2~4094 です。

- **disable**:DHCP クライアントが、指定された VLAN ID を音声 VLAN として使用しないように、指定された VLAN を無効にします。
- **enable**:DHCP クライアントが指定された VLAN ID を音声 VLAN として使用するように、VLAN がオンになっていることを指定します。

説明

voice-config コマンドを使用して、DHCP アドレスプールが DHCP クライアントに割り当てる Option 184 コンテンツを設定します。

undo voice-config コマンドは、DHCP アドレスプールが DHCP クライアントに割り当てた Option 184 の内容を削除するために使用します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#DHCP アドレスプール 0 に Option 184 の内容を指定します。ネットワークコールプロセッサの IP アドレスは 10.1.1.1、スタンバイサーバの IP アドレスは 10.2.2.2、音声 VLAN の ID は 3、オン、自動フェイルオーバーIP アドレスは 10.3.3.3、コール文字列は 99*です。

<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*

関連コマンド

- **display dhcp server pool**

目次

このセクションのページは **5-x-x** です。

14 章 DHCP リレー 14-1
14.1 DHCP リレー設定コマンド 14-1
14.1.1 dhcp relay client-information record 14-1
14.1.2 dhcp relay client-information refresh enable 14-2
14.1.3 dhcp relay information circuit-id 14-3
14.1.4 dhcp relay information enable 14-5
14.1.5 dhcp relay information remote-id 14-7
14.1.6 dhcp relay information strategy 14-8
14.1.7 dhcp relay release ip 14-9
14.1.8 dhcp relay server-address 14-10
14.1.9 display dhcp relay client-information 14-11
14.1.10 display dhcp relay information 14-14
14.1.11 display dhcp relay server-address 14-15
14.1.12 display dhcp relay statistics 14-17
14.1.13 reset dhcp relay client-information 14-19
14.1.14 reset dhcp relay statistics 14-19

14章 DHCP リレー

14.1 DHCPリレー設定コマンド

14.1.1 dhcp relay client-information record

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

デフォルト

DHCP リレーユーザアドレステーブルエントリロギング機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information record コマンドを使用すると、DHCP リレーユーザアドレステーブルエントリのロギングが有効になります。

undo dhcp relay client-information record コマンドは、DHCP リレーユーザアドレステーブルエントリのロギング機能を無効にするために使用します。

この DHCP クライアントのアドレステーブルエントリは、DHCP リレーが DHCP クライアントのゲートウェイデバイスとして機能する場合にのみ記録されます。DHCP リレーユーザアドレステーブルエントリには、DHCP クライアントの IP アドレス、MAC アドレス、ユーザアドレステーブルエントリタイプなどの情報が記録されます。

DHCP リレーのユーザアドレステーブルエントリの記録をオフにすると、DHCP リレーに記録されているすべてのアドレステーブルエントリが削除されます。

例

#DHCP リレーユーザアドレステーブルエントリのロギングを有効にします。

<Sysname> system-view
[Sysname] dhcp relay client-information record

関連コマンド

- **dhcp relay client-information refresh**
- **dhcp relay client-information refresh enable**

14.1.2 dhcp relay client-information refresh enable

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

デフォルト

DHCP リレー動的ユーザアドレステーブルエントリタイミングリフレッシュ機能はオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information refresh enable コマンドを使用して、DHCP リレー動的ユーザアドレステーブルエントリのタイミング更新機能を有効にします。

undo dhcp relay client-information refresh enable コマンドは、DHCP リレー動的ユーザアドレステーブルエントリのタイミング更新機能を無効にするために使用します。

DHCP クライアントは動的に取得した IP アドレスを解放すると、 DHCP サーバに DHCP-RELEASE メッセージをユニキャストで送信し、 DHCP リレーはそのメッセージの内容を処理しない。DHCP リレーにその IP アドレスと MAC アドレスのバインディング関係が記録されている場合、DHCP リレーのユーザアドレステーブルエントリはリアルタイムで更新されません。この問題を解決するために、DHCP リレーは動的ユーザアドレステーブルエントリのタイミングリフレッシュ機能をサポートします。

DHCP リレー動的ユーザアドレステーブルエントリタイミング更新機能がオンの場合、DHCP リレーは、クライアントが取得した IP アドレスと DHCP リレーインタフェースの MAC アドレスを使用して、指定された時間ごとに DHCP-REQUEST メッセージを DHCP サーバに送信します。

- DHCP リレーが DHCP サーバ応答の DHCP-ACK メッセージを受信した場合、または指定時間内に DHCP サーバ応答メッセージを受信しなかった場合、この IP アドレスはすでに割り当て可能であることを示し、DHCP リレーは動的ユーザアドレステーブルの対応するエントリを削除し、アドレスの浪費を避けるため、DHCP リレーは DHCP-ACK メッセージを受信した後、DHCP-RELEASE メッセージを送信して要求された IP アドレスを解放します。
- DHCP リレーが DHCP サーバ応答の DHCP-NAK メッセージを受信した場合、その IP アドレスのバインディング情報はまだ存在し、DHCP リレーはその IP アドレスのエントリを削除しません。

DHCP リレーの動的なユーザアドレステーブルエントリのタイミング更新機能をオフにすると、DHCP リレーに記録されたユーザアドレステーブルエントリが自動的にエージングされないことに注意してください。DHCP クライアントが要求された IP アドレスを解放したら、ユーザは **reset dhcp relay client-information** コマンドを実行して、DHCP リレー上の対応するユーザアドレステーブルエントリを削除する必要があります。

例

#DHCP リレー動的ユーザアドレステーブルエントリのタイミングリフレッシュ機能をオフにします。

<Sysname> system-view
[Sysname] undo dhcp relay client-information refresh enable

関連コマンド

- **dhcp relay client-information record**
- **dhcp relay client-information refresh**
- **reset dhcp relay client-information**

14.1.3 dhcp relay information circuit-id

Syntax

dhcp relay information circuit-id { **bas** [**sub-interface-vlan**] | **srv6-opcode** | **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] [**interface**] } [**sub-interface-vlan**] [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

デフォルト

パディングモードは normal で、パディング形式は hex です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

bas:Circuit ID サブオプションの入力に、MIB 仕様のフォーマットがサポートされていることを示します。*interface-type slot/subslot/port vxlan_id.vlan_id.subvlan_id* の形式でカプセル化されたインタフェース情報、VLAN 情報が入力されます。

sub-interface-vlan:L 2 VE サブインタフェースが存在する VLAN の VLAN 番号を Circuit ID サブオプションに設定します。このパラメータは、L 3 VE インタフェースでのみ使用

されます。このパラメータが指定されていない場合は、このコマンドが設定されているインタフェースの VLAN ID が入力されています。

srv6-opcode:インタフェース SRv6 SID の Opcode で Circuit ID サブオプションを設定するように指定します。この情報は、DHCPv6 サーバがアドレスとネットワークパラメータを割り当てるための基準として使用できます。

string *circuit-id*:Circuit ID サブオプションにユーザ設定の文字列を指定します。circuit-id は、Circuit ID サブオプションの内容を入力するようにユーザが設定した 3~63 文字の文字列で、大文字と小文字が区別されます。

normal:Circuit ID サブオプションを Normal モードで、VLAN ID とポート番号を指定します。

verbose:Circuit ID サブオプションを Verbose モードで指定します。入力されるのは、ノード ID、インタフェース情報、およびインタフェースが存在する VLAN 番号です。ノード ID デフォルトは、ノードの MAC アドレスで構成されます。インタフェース情報は、デフォルトで Ethernet タイプ(固定値「eth」)、ボックス番号、スロット番号、サブスロット番号、インタフェース番号で構成されます。

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }:アクセスノード ID を指定します。

- **mac**:ノードの MAC アドレスをノード識別子とすることを示す。
- **sysname**:ノードのデバイス名をノード ID として使用することを示します。デバイスのシステム名は、システム・ビューで sysname コマンドを使用して構成できます。設定されているパディング形式に関係なく、デバイスのシステム名は常に ASCII コード形式でパディングされます。
- **user-defined** *node-identifier*:ノード ID として指定された文字列を表します。node-identifier は 1~50 文字の文字列で、大文字と小文字が区別されます。設定されているパディング形式に関係なく、指定された文字列は常に ASCII コード形式でパディングされます。

interface:インタフェース情報をインタフェース名で構成することを示し、常に ASCII コード形式で入力する。

format:Circuit ID サブオプションのパディング形式を指定します。

ascii:Circuit ID サブオプションを ASCII コード形式で入力するように指定します。つまり、数値を対応する ASCII コードに変換して Circuit ID サブオプションに入力します。

hex:Circuit ID サブオプションを 16 進数で指定します。

説明

dhcp relay information circuit-id コマンドは、Option 82 の Circuit ID サブオプションのパディングモードとパディング形式を設定するために使用します。

undo dhcp relay information circuit-id コマンドを使用して、デフォルトの状態を復元します。

Circuit ID サブオプションを異なるモードで設定すると、設定形式が異なります。

- Circuit ID サブオプションにユーザ設定の文字列を入力する場合、入力形式は ASCII コード形式に固定されます。
- Circuit ID サブオプションを Normal および Verbose モードで設定する場合、設定形式はこのコマンドの設定によって決まります。

このコマンドでパディング形式が指定されていない場合、Normal モードでは、VLAN ID とポート番号の両方が hex 形式でパディングされます。Verbose モードの場合、ノード ID (MAC アドレス、デバイスのシステム名、または指定した文字列)、Ethernet タイプ、フレーム番号、スロット番号、サブスロット番号、インタフェース番号は ASCII コード形式で入力され、VLAN ID は hex 形式で入力されます。

- このコマンドで入力形式として ascii を指定した場合、すべてのコンテンツは ASCII コード形式で入力されます。
- このコマンドで hex 形式が指定されている場合、Normal モードでは VLAN ID とポート番号の両方が hex 形式で入力されます。Verbose モードの場合、デバイスのノード ID、Ethernet タイプは ASCII コード形式で入力され、残りは hex 形式で入力されます。
- デバイスのシステム名(sysname)をノード ID として DHCP メッセージの Option 82 に入力する場合、システム名にスペースを含めることはできません。そうでない場合、DHCP リレーは Option 82 の追加または置換に失敗します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#Option 82 を Verbose モードで入力する Circuit ID サブオプションを設定します。ノード ID はデバイスのシステム名で、入力形式は ASCII コード形式です。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information circuit-id verbose node-identifier sysname format ascii
```

関連コマンド

- **dhcp relay forward reply by-option82**
- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

14.1.4 dhcp relay information enable

Syntax

dhcp relay information enable

undo dhcp relay information enable

デフォルト

DHCP リレーサポート Option 82 機能はオフです。

View

Interface view

定義済みユーザロール

network-admin

説明

dhcp relay information enable コマンドは、Option 82 機能をサポートする DHCP リレーを有効にするために使用します。

undo dhcp relay information enable コマンドは、Option 82 機能をサポートする DHCP リレーをシャットダウンするために使用されます。

DHCP リレーサポート Option 82 機能を有効にすると、DHCP リレーは、DHCP サーバに転送される要求メッセージに Option 82 オプションを追加します。オプションの内容は、**dhcp relay information circuit-id** コマンドと **dhcp relay information remote-id** コマンドによって決まります。DHCP リレーが受信した要求メッセージに Option 82 オプションがすでに含まれている場合は、**dhcp relay information strategy** コマンドで設定されたポリシーに従って要求メッセージを処理します。

DHCP リレーが Option 82 機能をサポートしていない場合、DHCP リレーは、DHCP サーバに転送される要求メッセージに Option 82 オプションを追加したり、受信した要求メッセージに Option 82 オプションが含まれているかどうかをチェックしたりしません。

例

#DHCP リレーを有効にする Option 82 機能をサポートします。

<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable

関連コマンド

- **dhcp relay forward reply by-option82**
- **dhcp relay information circuit-id**
- **dhcp relay information remote-id**
- **dhcp relay information strategy**
- **display dhcp relay information**

14.1.5 dhcp relay information remote-id

Syntax

dhcp relay information remote-id { **normal** [**format** { **ascii** | **hex** }] | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

デフォルト

Option 82 の Remote ID サブオプションのパディングモードは Normal で、パディング形式は hex です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

normal:受信側メッセージインタフェースの MAC アドレスを入力するために、Remote ID サブオプションを Normal モードで指定します。

format:Remote ID サブオプションのパディング形式を指定します。このパラメータが設定されていない場合は、hex 形式で入力されます。

ascii:Remote ID サブオプションを ASCII コード形式で入力するように指定します。つまり、数値を対応する ASCII コードに変換して Remote ID サブオプションに入力します。

hex:Remote ID サブオプションを 16 進数で指定します。

string *remote-id*:Remote ID サブオプションにユーザ設定の文字列を指定します。remote-id は、Remote ID サブオプションの内容を入力するようにユーザが設定した 1~63 文字の文字列で、大文字と小文字が区別されます。

sysname:Remote ID サブオプションにデバイスのシステム名を指定します。デバイスのシステム名は、System view で sysname コマンドを使用して構成できます。

説明

dhcp relay information remote-id コマンドは、Option 82 の Remote ID サブオプションのパディングモードとパディング形式を設定するために使用します。

undo dhcp relay information remote-id コマンドを使用して、デフォルトの状態を復元します。

Remote ID サブオプションにユーザ設定の文字列(string)とデバイスのシステム名(sysname)を入力すると、入力は ASCII 形式に固定されます。Remote ID サブオプションを Normal モードで設定すると、このコマンドで設定した入力形式によって入力内容の形式が決まります。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#文字列 **device001** を Option 82 に設定する Remote ID サブオプションとしてパディングします。

<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy replace
[Sysname-Vlan-interface10] dhcp relay information remote-id string device001

関連コマンド

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

14.1.6 dhcp relay information strategy

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

デフォルト

DHCP リレーは、replace の Option 82 を持つ要求メッセージを処理します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

drop:メッセージに Option 82 が含まれている場合、そのメッセージを破棄する。

keep:メッセージに Option 82 が付いていれば、そのメッセージ中の Option 82 をそのまま転送する。

replace:メッセージに Option 82 が含まれている場合、Option 82 は設定されたパディングおよびパディングフォーマットでパディングされ、メッセージ内の Option 82 はこのオプションで置き換えられて転送されます。

説明

dhcp relay information strategy コマンドは、Option 82 を含む要求メッセージの DHCP リレー処理ポリシーを設定するために使用します。

undo dhcp relay information strategy コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、Option 82 を含むリクエストメッセージに対してのみ有効です。

DHCP リレーが Option 82 をサポートしている場合、DHCP リレーは、Option 82 を含まない要求メッセージを受信したときに、常に Option 82 を要求メッセージに追加して DHCP サーバに転送するように処理されます。

Option 82 要求メッセージを含む DHCP リレーの処理ポリシーが replace の場合、Option 82 のパディングモードとパディングフォーマットを設定する必要があります。処理ポリシーが keep または drop の場合、Option 82 オプションのパディングモードとパディング形式を設定する必要はありません。

例

#受信した要求メッセージに Option 82 が含まれている場合、 DHCP リレーはそのメッセージ中の Option 82 を保持したまま転送するように設定する。

<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay information enable
[Sysname-Vlan-interface10] dhcp relay information strategy keep

関連コマンド

- **dhcp relay information enable**
- **display dhcp relay information**

14.1.7 dhcp relay release ip

Syntax

dhcp relay release ip *ip-address*

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address:解放を要求している DHCP クライアントの IP アドレス。

説明

dhcp relay release ip コマンドは、クライアントが要求した IP アドレスの解放を DHCP サーバに要求するように設定します。

DHCP リレーにクライアント IP アドレスに対応する動的ユーザアドレステーブルエントリがある場合、DHCP リレーによってクライアント IP アドレスが解放されるように設定

すると、DHCP リレーは DHCP サーバに DHCP-RELEASE メッセージを送信します。DHCP サーバはこのメッセージを受信すると、指定された IP アドレスのバインド情報を解放します。DHCP リレーは、動的ユーザアドレステーブルエントリも削除します。

例

#クライアントが要求した IP アドレス 1.1.1.1 の解放を DHCP サーバに要求します。

<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1

14.1.8 dhcp relay server-address

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

デフォルト

DHCP リレーで DHCP サーバのアドレスが指定されていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address:DHCP サーバの IP アドレス。DHCP リレーは、DHCP クライアントが送信したメッセージをそのアドレスに転送します。

説明

dhcp relay server-address コマンドは、DHCP リレー上の DHCP サーバのアドレスを指定します。

undo dhcp relay server-address コマンドは、指定された DHCP サーバのアドレスを DHCP リレーから削除するために使用します。

指定された DHCP サーバの IP アドレスは、DHCP リレーのインタフェースの IP アドレスと同じネットワークセグメントに存在できません。そうしないと、クライアントが IP アドレスを取得できない可能性があります。

dhcp relay server-address コマンドを複数回実行すると、複数の DHCP サーバアドレスを指定できます。1 つのインタフェースに最大 8 つの DHCP サーバアドレスを指定できます。DHCP リレーは、 DHCP クライアントが送信したメッセージを受信すると、それをすべての DHCP サーバに転送する。

undo dhcp relay server-address コマンドの実行時に ip-address パラメータが指定されていない場合は、インタフェース上のすべての DHCP サーバアドレスが削除されます。

例

#VLAN インタフェース 10 の DHCP リレーの DHCP サーバアドレスを 1.1.1.1 に指定します。

<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] dhcp relay server-address 1.1.1.1

関連コマンド

- **dhcp select relay**
- **display dhcp relay interface**

14.1.9 display dhcp relay client-information

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースのユーザアドレステーブルエントリ情報を表示します。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。このパラメータが指定されていない場合は、すべてのインタフェースのユーザアドレステーブルエントリ情報が表示されます。

ip *ip-address*:指定した IP アドレスのユーザアドレステーブルエントリ情報を表示します。このパラメータが指定されていない場合は、すべての IP アドレスのユーザアドレステーブルエントリ情報が表示されます。

説明

DHCP リレーのユーザアドレステーブルエントリ情報を表示するには、**display dhcp relay client-information** コマンドを使用します。

DHCP リレーは、**dhcp relay client-information record** コマンドを実行するまで、ユーザアドレステーブルエントリ情報を記録しません。

例

#すべての DHCP リレーのユーザアドレステーブルエントリ情報を表示します。

<Sysname> display dhcp relay client-information

Total number of client-information items: 2

Total number of dynamic items: 1

Total number of temporary items: 1

IP address	MAC address	Type	Interface	VPN name
10.1.1.1	00e0-0000-0001	Dynamic	Vlan2	N/A
10.1.1.5	00e0-0000-0000	Temporary	Vlan2	N/A

#DHCP リレーの指定されたアドレスのユーザアドレステーブルエントリ情報を表示します。

<Sysname> display dhcp relay client-information ip 10.1.1.5

Total number of client-information items: 1

Total number of dynamic items: 1

Total number of temporary items: 0

IP address : 10.1.1.5

MAC address : 00e0-0000-0000

Type : Dynamic

Port index : N/A

Interface : Vlan2

VPN name : N/A

Server address : 12.1.1.2

Access type : CommonV4

Outer VLAN : N/A

Inner VLAN : N/A

PPP index : 0

表 14-1　display dhcp relay client-information コマンドの表示情報の説明

フィールド	説明
Total number of client-information items	ユーザーアドレス情報エントリの合計数
Total number of dynamic items	動的ユーザアドレスエントリの合計数
Total number of temporary items	一時ユーザアドレスエントリの合計数
IP address	DHCPクライアントのIPアドレス
MAC address	DHCPクライアントのMACアドレス

フィールド	説明
Type	ユーザアドレステーブルのエントリタイプには、次の値があります。 • Dynamic:動的ユーザアドレステーブルエントリ DHCP クライアント REQUEST 要求に対する DHCP サーバからの ACK 応答を受信したときに作成されるユーザテーブルエントリ • Temporary:一時ユーザアドレステーブルエントリ。DHCP クライアントから REQUEST 要求を受信したが、DHCP サーバ ACK 応答を受信しなかった場合に作成されるユーザテーブルエントリ。
Interface	DHCPクライアントに接続する3層インタフェース。ユーザアドレステーブルエントリにインタフェースが記録されていない場合は、 「N/A」 と表示されます。
VPN name	(未サポート) VPNインスタンス名。テーブルエントリがどのVPNにも属していない場合は 「N/A」 と表示されます。
Port index	DHCPリレーDHCPクライアント要求メッセージを受信するレイヤ2ポート情報。メッセージがレイヤ2ポートからDHCPリレーに入らない場合は、"N/A"と表示されます。
Server address	DHCPサーバアドレス
Access type	アクセスタイプ。次の値があります。 • CommonV4:Portal アクセス方式または DHCP アドレス要求方式
Outer VLAN	DHCPリレーユーザアドレステーブルエントリの外側のレイヤVLAN Tagが存在しない場合は、N/Aと表示されます。
Inner VLAN	DHCPリレーユーザアドレステーブルエントリの内部レベルVLAN Tagが存在しない場合は、N/Aと表示されます。
PPP index	(未サポート)ユーザアドレステーブルエントリのPPPインデックス。存在しない場合はN/Aと表示されます。

関連コマンド

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

14.1.10 display dhcp relay information

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースの Option 82 設定情報を表示します。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。このパラメータを指定しない場合は、すべてのインタフェースの Option 82 構成情報が表示されます。

説明

display dhcp relay information コマンドは、DHCP リレーの Option 82 設定情報を表示するために使用します。

例

#すべてのインタフェースの Option 82 設定情報を表示します。

<Sysname> display dhcp relay information
Interface: Vlan-interface100
Status: Enable
Strategy: Replace
Circuit ID Pattern: Verbose
Remote ID Pattern: Sysname
Circuit ID format: Undefined
Remote ID format: ASCII
Node identifier: aabbcc
Interface: Vlan-interface200
Status: Enable
Strategy: Replace
Circuit ID Pattern: User Defined
Remote ID Pattern: User Defined
Circuit ID format: ASCII
Remote ID format: ASCII
User defined:

Circuit ID: vlan100

Remote ID: device001

表 14-2 display dhcp relay information コマンドの表示情報の説明

フィールド	説明
Interface	インタフェース名
Status	Option 82のステータス。値は次のとおりです。 • Enable:DHCP リレーサポートを有効にする Option 82 機能 • Disable:DHCP リレーが有効になっていない Option 82 機能のサポート
Strategy	Option 82を含むリクエストメッセージの処理ポリシー。値はDrop、Keep、またはReplaceです。
Circuit ID Pattern	Circuit IDサブオプションは、Verbose、Normal、Srv6-opcode、User Definedのいずれかの値で移入されます。
Remote ID Pattern	Remote IDサブオプションは、Sysname、NormalまたはUser Definedのいずれかの値で移入されます。
Circuit ID format	Circuit IDサブオプションには、ASCII、Hex、Undefinedのいずれかの値を入力します。
Remote ID format	Remote IDサブオプションには、ASCII、Hex、Undefinedのいずれかの値を入力します。
Node identifier	アクセスノードの識別
User defined	ユーザ定義のサブオプションの内容
Circuit ID	ユーザ定義のCircuit IDサブオプションの内容
Remote ID	ユーザ定義のRemote IDサブオプションの内容

14.1.11 display dhcp relay server-address

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースの DHCP サーバアドレス情報を表示します。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。このパラメータを指定しない場合は、すべてのインタフェースの DHCP サーバアドレス情報が表示されます。

説明

display dhcp relay server-address コマンドは、インタフェースで指定された DHCP サーバアドレス情報を表示します。

例

#すべてのインタフェースで指定されている DHCP サーバアドレス情報を表示します。

<Sysname> display dhcp relay server-address

Interface name Server IP address

Vlan2 2.2.2.2

#VLAN インタフェース 2 で指定された DHCP サーバアドレス情報を表示します。

<Sysname> display dhcp relay server-address interface vlan-interface 2

Active server address: 2.2.2.2

Interface name Server IP address

Vlan2 2.2.2.2

表 14-3　display dhcp relay server-address コマンドの表示情報の説明

フィールド	説明
Active server address:	次の値を持つ現在アクティブなDHCPサーバアドレス。 • [All] と表示されている場合は、現在構成されている DHCP サーバがすべての方法で選択されていることを示します。つまり、DHCP リレーはすべての DHCP サーバに同時に DHCP 要求メッセージを転送します。 • IP アドレスが表示されている場合は、現在構成されている DHCP サーバの選択モードがプライマリモードであり、そのアドレスが現在アクティブな DHCP サーバアドレスであることを示します。つまり、DHCP リレーは、そのアドレスに対応する DHCP サーバに DHCP 要求メッセージを転送します。
Interface name	インタフェース名
Server IP address	指定されたDHCPサーバアドレス

関連コマンド

- **dhcp relay server-address**

14.1.12 display dhcp relay statistics

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースの DHCP リレー関連のメッセージ統計情報を表示します。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。このパラメータが指定されていない場合は、すべての DHCP リレー関連のメッセージ統計情報が表示されます。

説明

display dhcp relay statistics コマンドを使用して、DHCP リレーに関するメッセージ統計情報を表示します。

例

#すべての DHCP リレー関連メッセージの統計情報を表示します。

```
<Sysname> display dhcp relay statistics
DHCP packets dropped:                   0
DHCP packets received from clients:     0
    DHCPDISCOVER:                       0
    DHCPREQUEST:                        0
    DHCPINFORM:                         0
    DHCPRELEASE:                        0
    DHCPDECLINE:                        0
    BOOTPREQUEST:                       0
DHCP packets received from servers:     0
    DHCPOFFER:                          0
    DHCPACK:                            0
    DHCPNAK:                            0
    BOOTPREPLY:                         0
DHCP packets relayed to servers:        0
    DHCPDISCOVER:                       0
    DHCPREQUEST:                        0
```

```
    DHCPINFORM:                 0
    DHCPRELEASE:                0
    DHCPDECLINE:                0
    BOOTPREQUEST:               0
DHCP packets relayed to clients:    0
    DHCPOFFER:                  0
    DHCPACK:                    0
    DHCPNAK:                    0
    BOOTPREPLY:                 0
DHCP packets sent to servers:       0
    DHCPDISCOVER:               0
    DHCPREQUEST:                0
    DHCPINFORM:                 0
    DHCPRELEASE:                0
    DHCPDECLINE:                0
    BOOTPREQUEST:               0
DHCP packets sent to clients:       0
    DHCPOFFER:                  0
    DHCPACK:                    0
    DHCPNAK:                    0
    BOOTPREPLY:                 0
```

表 14-4 display dhcp relay statistics コマンドの表示情報の説明

フィールド	説明
DHCP packets dropped	DHCPリレーがドロップしたメッセージ数
DHCP packets received from clients	DHCPリレークライアントから受信したDHCPメッセージの数
DHCP packets received from servers	DHCPリレーサーバから受信したDHCPメッセージの数
DHCP packets relayed to servers	DHCPリレーがサーバに転送するメッセージ数
DHCP packets relayed to clients	DHCPリレーがクライアントに転送するメッセージの数
DHCP packets sent to servers	動的なユーザアドレステーブルエントリの定期的な更新のために、DHCPリレーによってアクティブにサーバに送信されるDHCPメッセージの数
DHCP packets sent to clients	DHCPリレーがアクティブにクライアントに送信するDHCPメッセージの数(現在のデバイスがDHCPリレーとして動作している場合、DHCPメッセージはクライアントにプロアクティブに送信されません。)

関連コマンド

- **reset dhcp relay statistics**

14.1.13 reset dhcp relay client-information

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*:指定したインタフェースの DHCP リレーのユーザアドレステーブルエントリ情報をクリアします。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。このパラメータが指定されていない場合は、すべてのインタフェースの DHCP リレーのユーザアドレステーブルエントリ情報がクリアされます。

ip *ip-address*:指定した IP アドレスのユーザアドレステーブルエントリ情報をクリアします。このパラメータを指定しない場合は、すべての IP アドレスの DHCP リレーのユーザアドレステーブルエントリ情報がクリアされます。

説明

reset dhcp relay client-information コマンドは、DHCP リレーのユーザアドレステーブルエントリ情報をクリアするために使用します。

例

#すべての DHCP リレーのユーザアドレステーブルエントリ情報をクリアします。

<Sysname> reset dhcp relay client-information

関連コマンド

- **display dhcp relay client-information**

14.1.14 reset dhcp relay statistics

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*:指定したインタフェースの DHCP リレー関連のメッセージ統計情報をクリアします。interface-type interface-number はインタフェースタイプおよびインタフェース番号です。このパラメータが指定されていない場合は、すべての DHCP リレー関連のメッセージ統計情報がクリアされます。

説明

reset dhcp relay statistics コマンドは、DHCP リレーの関連するメッセージ統計情報をクリアするために使用されます。

例

#すべての DHCP リレー関連のメッセージ統計情報をクリアします。

<Sysname> reset dhcp relay statistics

関連コマンド

- **display dhcp relay statistics**

目次

このセクションのページは **5-x-x** です。

15 章 DHCP クライアント 15-1
15.1 DHCP クライアント設定コマンド 15-1
15.1.1 dhcp client dad enable 15-1
15.1.2 dhcp client dscp 15-1
15.1.3 display dhcp client 15-2
15.1.4 ip address dhcp-alloc 15-5

15章 DHCP クライアント

15.1 DHCPクライアント設定コマンド

15.1.1 dhcp client dad enable

Syntax

dhcp client dad enable

undo dhcp client dad enable

デフォルト

アドレス競合チェック機能がオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

dhcp client dad enable コマンドは、アドレス競合チェック機能を有効にします。

undo dhcp client dad enable コマンドは、アドレス競合チェック機能をオフにします。

DHCP クライアントは ARP メッセージを送受信することで、 DHCP サーバが割り当てた IP アドレスに対してアドレス衝突検出を行い、攻撃者がアドレス所有者になりすまして ARP 応答を行えば、 DHCP クライアントをだまして、 DHCP クライアントが割り当てられた IP アドレスを正常に使用できないようにすることができる。上記のような攻撃者がネットワーク内に存在する場合は、クライアントでアドレス競合チェック機能をオフにすることが推奨される。

例

#アドレス競合チェックをオフにします。

<Sysname> system-view
[Sysname] undo dhcp client dad enable

15.1.2 dhcp client dscp

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

デフォルト

DHCP クライアントが DHCP メッセージを送信する DSCP プライオリティは 56 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value:DHCP 要求メッセージの DSCP 優先度。範囲は 0~63 です。

説明

dhcp client dscp コマンドを使用して、DHCP クライアントが DHCP メッセージを送信する DSCP プライオリティを設定します。

undo dhcp client dscp コマンドを使用して、デフォルトの状態を復元します。

DSCP 優先度は、メッセージ自体の優先度を表し、メッセージ転送の優先度を決定する。DSCP 優先度の設定値が大きいほど、メッセージの優先度が高くなります。

例

#DHCP クライアントが送信する DHCP メッセージの DSCP プライオリティを 30 に設定します。

<Sysname> system-view
[Sysname] dhcp client dscp 30

15.1.3 display dhcp client

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose:DHCP クライアントの詳細を表示します。このパラメータが指定されていない場合は、DHCP クライアントの概要が表示されます。

interface *interface-type interface-number*:指定したインタフェースの DHCP クライアントに関する情報を表示します。interface-type interface-number はインターフェイスタイプおよびインタフェース番号です。このパラメータを指定しない場合は、すべてのインタフェースの DHCP クライアント情報が表示されます。

説明

display dhcp client コマンドを使用して、DHCP クライアントに関する情報を表示します。

例

#すべてのインタフェースの DHCP クライアントの簡単な情報を表示します。

<Sysname> display dhcp client

```
Vlan-interface10 DHCP client information:
  Current state: BOUND
  Allocated IP: 40.1.1.20 255.255.255.0
  Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
  DHCP server: 40.1.1.2
```

#すべてのインタフェースの DHCP クライアントの詳細を表示します。

<Sysname> display dhcp client verbose

```
Vlan-interface10 DHCP client information:
  Current state: BOUND
  Allocated IP: 40.1.1.20 255.255.255.0
  Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
  Lease from May 21 19:00:29 2012      to      May 31 19:00:29 2012
  DHCP server: 40.1.1.2
  Transaction ID: 0x1c09322d
  Default router: 40.1.1.2
Classless static routes:
     Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
     Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
  DNS servers: 44.1.1.11 44.1.1.12
  Domain name: ddd.com
  Boot servers: 200.200.200.200    1.1.1.1
  ACS parameter:
     URL: http://192.168.1.1:7547/acs
     Username: bims
     Password: ******
  Client ID type: acsii(type value=00)
  Client ID value: 000c.29d3.8659-Vlan10
  Client ID (with type) hex: 0030-3030-632e-3239-
                             6433-2e38-3635-392d-
                             4574-6830-2f30-2f32
```

T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.

表 15-1 display dhcp client コマンドの表示情報の説明

フィールド	説明
XXXX DHCP client information	DHCPクライアントとしてのインタフェース情報
Current state	DHCPクライアントステートマシンの現在の状態。値は次のとおりです。 • HALT: クライアントは IP アドレスの申請を停止します。 • INIT INIT:初期化状態です。 • SELECTING:DHCP-DISCOVER メッセージを送信して DHCP サーバを探した後、この状態になり、 DHCP サーバからの応答メッセージを待ちます。 • REQUESTING:DHCP-REQUEST メッセージを送信して IP アドレスを要求すると、この状態になり、 DHCP サーバからの応答メッセージを待ちます。 • BOUND:DHCP サーバから送信された DHCP-ACK メッセージを受信し、 IP アドレスの取得に成功すると、この状態になります。 • RENEWING:T 1 タイマタイムアウト後、この状態になります。 • REBOUNDING:T 2 タイマがタイムアウトしたら、この状態になります。
Allocated IP	DHCPサーバがインタフェースに割り当てるIPアドレス
Allocated lease	レンタル期間
T1	DHCPクライアントのリース時間の約半分(秒単位)
T2	DHCPクライアントのリース期間が7/8 (秒単位)
Lease from .... to	リース開始から終了までの時間
DHCP server	選択したDHCPサーバのアドレス
Transaction ID	DHCPクライアントが要求を開始するときに生成される乱数。要求プロセスを一意に識別します。
Default router	DHCPクライアントに指定されたゲートウェイアドレス
Classless static routes	DHCPクライアントに指定された分類されていない静的ルート
Static routes	DHCPクライアントに指定されたクラス化された静的ルート
DNS servers	DHCPクライアントに指定されたDNSサーバアドレス
Domain name	DHCPクライアントに指定されたドメイン名サフィックス
Boot servers	DHCPクライアントに指定されたPXEブートサーバーのアドレス。Option 43から最大16個のアドレスを取得できます。

フィールド	説明
ACS parameter	ACSパラメータ
URL	ACSのURLアドレス
Username	ACSデバイスへのログインに使用するユーザ名
Password	ACSアプライアンスへのログインに使用されるパスワード。存在する場合は「******」と表示されます。パスワードが存在しない場合は表示されません。
Client ID type	DHCPクライアントIDのタイプ。type valueはタイプ値を表します。タイプがASCIIの場合、type valueは00;MAC addressの場合、type valueは01;Hexの場合、type valueは設定された16進数の最初の2桁です。
Client ID value	DHCPクライアントIDの取得
Client ID (with type) hex	DHCPクライアントIDの16進数形式(タイプ値付きフィールド)
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	T 1タイマが期限切れになるまでの時間(約半分のレンタル時間)

関連コマンド

- **dhcp client identifier**
- **ip address dhcp-alloc**

15.1.4 ip address dhcp-alloc

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

デフォルト

インタフェースは、DHCP プロトコルを使用して IP アドレスを取得しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ip address dhcp-alloc コマンドは、DHCP プロトコルを使用して IP アドレスを取得するようにインタフェースを設定するために使用します。

undo ip address dhcp-alloc コマンドは、DHCP プロトコルを使用してインタフェースから取得した IP アドレスを取り消すために使用します。

インタフェースが DHCP プロトコルを使用して IP アドレスを取得すると、DHCP クライアントは DHCP-RELEASE メッセージを送信して DHCP サーバにリースを解放するように通知します。この時点でインタフェースがダウンしている場合、メッセージが正常に送信される保証はありません。

サブインターフェイスが DHCP プロトコルを使用して IP アドレスを取得するように設定されている場合、DHCP クライアントは、プライマリインターフェイスで shutdown コマンドを実行しても、サブインターフェイスの IP アドレスリースの解放を要求する DHCP-RELEASE メッセージを送信しません。

例

#VLAN インタフェース 10 でのインタフェースの設定 DHCP プロトコルを使用して IP アドレスを取得します。

<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address dhcp-alloc

関連コマンド

- **display dhcp client**

目次

このセクションのページは **5-x-x** です。

16 章 BOOTP クライアント 16-1
16.1 BOOTP クライアント設定コマンド 16-1
16.1.1 display bootp client 16-1
16.1.2 ip address bootp-alloc 16-2

16章 BOOTP クライアント

16.1 BOOTPクライアント設定コマンド

16.1.1 display bootp client

Syntax

display bootp client [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースのBOOTPクライアント関連情報を表示します。interface-type interface-number はインターフェイスタイプおよびインタフェース番号です。このパラメータを指定しない場合、すべてのインタフェース上の BOOTP クライアントに関する情報が表示されます。

説明

display bootp client コマンドは、BOOTP クライアントに関する情報を表示するために使用します。

例

#VLAN インタフェース 10 の BOOTP クライアント関連情報を表示します。

<Sysname> display bootp client interface vlan-interface 10

```
Vlan-interface10 BOOTP client information:
Allocated IP:169.254.0.2 255.255.0.0
Transaction ID:0 x3d8a7431
MAC Address:00 e0-fc0a-c3ef
```

表 16-1　display bootp client コマンドの表示情報の説明

フィールド	説明
XXXX BOOTP client information	BOOTPクライアントとしてのインタフェース情報
Allocated IP	BOOTPサーバがBOOTPクライアントに割り当てるIPアドレス

フィールド	説明
Transaction ID	BOOTPメッセージのXIDフィールド値は、BOOTPクライアントがBOOTP要求メッセージを送信するときに選択する乱数であり、BOOTPサーバの応答メッセージに一致します。応答メッセージのXIDフィールド値が要求メッセージのXIDフィールド値と異なる場合、BOOTPクライアントは応答メッセージを破棄します。
MAC Address	BOOTPクライアントのMACアドレス

関連コマンド

- **ip address bootp-alloc**

16.1.2 ip address bootp-alloc

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

デフォルト

インタフェースは、BOOTP プロトコルを使用して IP アドレスを取得しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ip address bootp-alloc コマンドは、BOOTP プロトコルを使用して IP アドレスを取得するようにインタフェースを設定するために使用します。

例

#VLAN インタフェース 10 でのインタフェースの設定 BOOTP プロトコルを使用して IP アドレスを取得します。

<Sysname> system-view

[Sysname] interface vlan-interface 10

[Sysname-Vlan-interface10] ip address bootp-alloc

関連コマンド

- **display bootp client**

目次

このセクションのページは **5-x-x** です。

17 章 DHCP スヌーピング 17-1
17.1 DHCP スヌーピング設定コマンド 17-1
17.1.1 dhcp snooping binding record 17-1
17.1.2 dhcp snooping enable 17-2
17.1.3 dhcp snooping information circuit-id 17-3
17.1.4 dhcp snooping information enable 17-5
17.1.5 dhcp snooping information remote-id 17-6
17.1.6 dhcp snooping information strategy 17-7
17.1.7 dhcp snooping trust 17-9
17.1.8 display dhcp snooping binding 17-10
17.1.9 display dhcp snooping information 17-11
17.1.10 display dhcp snooping packet statistics 17-13
17.1.11 display dhcp snooping trust 17-14
17.1.12 reset dhcp snooping binding 17-16
17.1.13 reset dhcp snooping packet statistics 17-16

17章 DHCP スヌーピング

17.1 DHCPスヌーピング設定コマンド

🕮 **メモ** :

DHCP スヌーピングは、DHCP クライアントと DHCP サーバ間、または DHCP クライアントと DHCP リレーエージェント間で機能します。DHCP サーバと DHCP リレーエージェント間では機能しません。

17.1.1 dhcp snooping binding record

Syntax

dhcp snooping binding record

undo dhcp snooping binding record

デフォルト

ポート DHCP Snooping テーブルエントリのロギングがオフになっています。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

VLAN view

定義済みユーザロール

network-admin

説明

dhcp snooping binding record コマンドは、ポートの DHCP Snooping テーブルエントリロギング機能をオンにするために使用します。

undo dhcp snooping binding record コマンドは、ポートの DHCP Snooping テーブルエントリロギング機能をオフにします。

ユーザは、DHCP Snooping デバイスがクライアントに直接接続するポートで、DHCP Snooping テーブルエントリのロギングを有効にできます。

ポートで DHCP Snooping テーブルエントリのロギングが有効になると、デバイスはそのポートで受信されたメッセージを受信して DHCP Snooping テーブルエントリを生成します。

例

#ポート GigabitEthernet1/0/1 の DHCP Snooping テーブルエントリロギングを有効にします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping binding record

17.1.2 dhcp snooping enable

Syntax

dhcp snooping enable

undo dhcp snooping enable

デフォルト

グローバル DHCP Snooping 機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

dhcp snooping enable コマンドは、DHCP Snooping 機能をグローバルに有効にするために使用します。

undo dhcp snooping enable コマンドは、DHCP Snooping 機能をグローバルに停止するために使用します。

DHCP Snooping がグローバルに有効になっている場合、信頼できないポートが DHCP サーバから送信されたメッセージを受信すると、クライアントが正当な DHCP サーバから IP アドレスを取得できるように、そのメッセージは破棄されます。

グローバル DHCP Snooping 機能をオフにすると、すべてのポートが DHCP サーバの応答メッセージを転送します。

例

#DHCP Snooping をグローバルに有効にします。

<Sysname> system-view
[Sysname] dhcp snooping enable

17.1.3 dhcp snooping information circuit-id

Syntax

dhcp snooping information circuit-id { [**vlan** *vlan-id*] **string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] } [**format** { **ascii** | **hex** }] }

undo dhcp snooping information circuit-id [**vlan** *vlan-id*]

デフォルト

Option 82 の Circuit ID サブオプションの塗りパターンは Normal で、塗りフォーマットは hex です。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*:指定した VLAN 内から受信した DHCP メッセージに Circuit ID サブオプションを設定します。このパラメータが指定されていない場合、デフォルト VLAN 内で受信された DHCP メッセージには、Circuit ID サブオプションが設定されます。

string *circuit-id*:Circuit ID サブオプションにユーザ設定の文字列を指定します。circuit-id は、Circuit ID サブオプションの内容を入力するようにユーザが設定した 3~63 文字の文字列で、大文字と小文字が区別されます。

normal:Circuit ID サブオプションを Normal モードで、VLAN ID とポート番号を指定します。

verbose:Circuit ID サブオプションを Verbose モードで指定します。入力されるのは、ノード ID、インタフェース情報、およびインタフェースが存在する VLAN 番号です。ノード ID デフォルトは、ノードの MAC アドレスで構成されます。インタフェース情報は、デフォルトで Ethernet タイプ(固定値「eth」)、ボックス番号、スロット番号、サブスロット番号、インタフェース番号で構成されます。

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }:アクセスノードの ID を指定します。

- **mac**:ノードの MAC アドレスをノード識別子とすることを示す。
- **sysname**:ノードのデバイス名をノード ID として使用することを示します。デバイスのシステム名は、System view で sysname コマンドを使用して構成できます。設定されているパディング形式に関係なく、デバイスのシステム名は常に ASCII コード形式でパディングされます。

- **user-defined** *node-identifier*:ノード ID として指定された文字列を表します。node-identifier は 1~50 文字の文字列で、大文字と小文字が区別されます。設定されているパディング形式に関係なく、指定された文字列は常に ASCII コード形式でパディングされます。

format:Circuit ID サブオプションのパディング形式を指定します。

ascii:Circuit ID サブオプションを ASCII コード形式で入力するように指定します。つまり、数値を対応する ASCII コードに変換して Circuit ID サブオプションに入力します。

hex:Circuit ID サブオプションを 16 進数で指定します。

説明

dhcp snooping information circuit-id コマンドは、Option 82 の Circuit ID サブオプションのパディングモードとパディング形式を設定するために使用します。

undo dhcp snooping information circuit-id コマンドを使用して、デフォルトの状態を復元します。

Circuit ID サブオプションにユーザ設定の文字列を入力すると、入力形式は ASCII コード形式に固定されます。

Circuit ID サブオプションを Normal および Verbose モードで設定する場合、設定形式はこのコマンドの設定によって決まります。

- このコマンドでパディング形式が指定されていない場合、Normal モードでは、VLAN ID とポート番号の両方が hex 形式でパディングされます。Verbose モードの場合、ノード ID (MAC アドレス、デバイスのシステム名、または指定した文字列)、Ethernet タイプ、フレーム番号、スロット番号、サブスロット番号、インタフェース番号は ASCII コード形式で入力され、VLAN ID は hex 形式で入力されます。
- このコマンドで入力形式として ascii を指定した場合、すべてのコンテンツは ASCII コード形式で入力されます。
- このコマンドで hex 形式が指定されている場合、Normal モードでは VLAN ID とポート番号の両方が hex 形式で入力されます。Verbose モードの場合、デバイスのノード ID、Ethernet タイプは ASCII コード形式で入力され、残りは hex 形式で入力されます。

デバイスのシステム名(sysname)をノード ID として DHCP メッセージの Option 82 に入力する場合、システム名にスペースを含めることはできません。それ以外の場合、DHCP Snooping は Option 82 の追加または置換に失敗します。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#Option 82 を Verbose モードで入力する Circuit ID サブオプションを設定します。ノード ID はデバイスのシステム名で、入力形式は ASCII コード形式です。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy replace
```

[Sysname-GigabitEthernet1/0/1] dhcp snooping information circuit-id verbose node-identifier sysname format ascii

関連コマンド

- **dhcp snooping information enable**
- **dhcp snooping information strategy**
- **display dhcp snooping information**

17.1.4 dhcp snooping information enable

Syntax

dhcp snooping information enable

undo dhcp snooping information enable

デフォルト

DHCP Snooping サポート Option 82 機能はオフです。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

dhcp snooping information enable コマンドは、Option 82 機能をサポートする DHCP Snooping を開くために使用します。

undo dhcp snooping information enable コマンドは、Option 82 機能をサポートする DHCP Snooping を閉じるために使用します。

DHCP Snooping を有効にして Option 82 をサポートすると、DHCP Snooping は DHCP サーバに転送される要求メッセージに Option 82 オプションを追加します。オプションの内容は、dhcp snooping information circuit-id と dhcp snooping information remote-id によって決まります。DHCP Snooping が受信した要求メッセージに Option 82 オプションがすでに含まれている場合は、dhcp snooping information strategy で設定されたポリシーに従って要求メッセージを処理します。

例

#DHCP Snooping を有効にする Option 82 機能をサポートします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable

関連コマンド

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**
- **dhcp snooping information strategy**

17.1.5 dhcp snooping information remote-id

Syntax

dhcp snooping information remote-id { **normal** [**format** { **ascii** | **hex** }] | [**vlan** *vlan-id*] { **string** *remote-id* | **sysname** } }

undo dhcp snooping information remote-id [**vlan** *vlan-id*]

デフォルト

Option 82 の Remote ID サブオプションのパディングモードは Normal で、パディング形式は hex です。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*:指定した VLAN 内から受信した DHCP メッセージに Remote ID サブオプションを設定します。このパラメータが指定されていない場合、デフォルト VLAN 内で受信された DHCP メッセージには、Remote ID サブオプションが設定されます。

string *remote-id*:Remote ID サブオプションにユーザ設定の文字列を指定します。remote-id は、Remote ID サブオプションの内容を入力するようにユーザが設定した 1~63 文字の文字列で、大文字と小文字が区別されます。

sysname:Remote ID サブオプションにデバイスのシステム名を指定します。デバイスのシステム名は、System view で sysname コマンドを使用して構成できます。

normal:受信側メッセージインターフェイスの MAC アドレスを入力するために、Remote ID サブオプションを Normal モードで指定します。

format:Remote ID サブオプションのパディング形式を指定します。このパラメータが指定されていない場合は、hex モードで入力されます。

ascii:Remote ID サブオプションを ASCII コード形式で入力するように指定します。つまり、数値を対応する ASCII コードに変換して Remote ID サブオプションに入力します。

hex:Remote ID サブオプションを 16 進数で指定します。

説明

dhcp snooping information remote-id コマンドは、Option 82 の Remote ID サブオプションのパディングモードとパディング形式を設定するために使用します。

undo dhcp snooping information remote-id コマンドを使用して、デフォルトの状態を復元します。

Remote ID サブオプションにユーザ設定の文字列(string)とデバイスのシステム名(sysname)を入力すると、入力は ASCII 形式に固定されます。Remote ID サブオプションを Normal モードで設定すると、このコマンドで設定した入力形式によって入力内容の形式が決まります。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#文字列 device001 を Option 82 に設定する Remote ID サブオプション。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy replace
[Sysname-GigabitEthernet1/0/1] dhcp snooping information remote-id string device001

関連コマンド

- **dhcp snooping information enable**
- **dhcp snooping information strategy**
- **display dhcp snooping information**

17.1.6 dhcp snooping information strategy

Syntax

dhcp snooping information strategy { **append** | **drop** | **keep** | **replace** }

undo dhcp snooping information strategy

デフォルト

Option 82 を持つリクエストメッセージの処理ポリシーは replace です。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

append:メッセージを次のように処理して転送します。

- メッセージに Option 82 が含まれていない場合は、設定された塗りつぶしモードに従って Option 82 が設定されます。
- メッセージに Option 82 が含まれている場合:
  - **dhcp snooping information vendor-specific** コマンドが設定されている場合は、このコマンドの設定に従って、Option 82 の Vendor-specific サブオプションにコンテンツを追加します。
  - **dhcp snooping information vendor-specific** コマンドが設定されていない場合、メッセージ内の Option 82 は変更されません。

drop:メッセージに Option 82 が含まれている場合、そのメッセージを破棄する。

keep:メッセージに Option 82 が付いていれば、そのメッセージ中の Option 82 をそのまま転送する。

replace:メッセージに Option 82 が含まれているかどうかにかかわらず、配置されたパディングパターンに従って Option 82 をパディングし、メッセージ中の既存の Option 82 をこのオプションに置き換えて転送する。

説明

dhcp snooping information strategy コマンドを使用して、Option 82 を含むリクエストメッセージに対する DHCP Snooping の処理ポリシーを設定します。

undo dhcp snooping information strategy コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、Option 82 を含むリクエストメッセージに対してのみ有効です。

DHCP Snooping が Option 82 をサポートするように設定されている場合、DHCP Snooping は常に、Option 82 を含まない受信した要求メッセージに Option 82 を追加し、DHCP サーバに転送するように処理されます。

DHCP Snooping Option 82 要求メッセージを含む処理ポリシーが replace の場合、Option 82 の入力モードと入力フォーマットを設定する必要があります。処理ポリシーが keep または drop の場合、Option 82 オプションのパディングモードとパディング形式を設定する必要はありません。

例

#設定 DHCP Snooping Option 82 を使用してリクエストメッセージに keep ポリシーを使用します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping information enable
[Sysname-GigabitEthernet1/0/1] dhcp snooping information strategy keep
```

関連コマンド

- **dhcp snooping information circuit-id**
- **dhcp snooping information remote-id**
- **dhcp snooping information vendor-specific**

17.1.7 dhcp snooping trust

Syntax

dhcp snooping trust

undo dhcp snooping trust

デフォルト

DHCP Snooping 機能を有効にすると、デバイス上の DHCP Snooping 機能をサポートするすべてのポートが信頼できないポートになります。

View

Layer 2 Ethernet interface

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

dhcp snooping trust コマンドを使用して、ポートを信頼ポートとして設定します。

undo dhcp snooping trust コマンドは、信頼されていないポートにポートを復元するために使用します。

DHCP サーバの方向を向いているポートは信頼できるポートに設定し、他のポートは信頼できないポートに設定する必要があります。これにより、DHCP クライアントは正当な DHCP サーバからしか IP アドレスを取得できず、プライベートに作成された仮想 DHCP サーバは DHCP クライアントに IP アドレスを割り当てることができません。

例

#3 層イーサネットインターフェイス GigabitEthernet1/0/1 を信頼ポートとして設定します。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dhcp snooping trust
```

関連コマンド

- **display dhcp snooping trust**

17.1.8 display dhcp snooping binding

Syntax

display dhcp snooping binding [**ip** *ip-address* [**vlan** *vlan-id*]] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*:指定した IP アドレスの DHCP Snooping テーブルエントリ情報を表示します。

vlan *vlan-id*:指定した VLAN 内の DHCP Snooping テーブルエントリ情報を表示します。

verbose:DHCP Snooping テーブルエントリの詳細を表示します。このパラメータが指定されていない場合は、DHCP Snooping 表エントリのサマリー情報が表示されます。

説明

display dhcp snooping binding コマンドは、DHCP Snooping テーブルエントリ情報を表示します。

ip ip-address および vlan vlan-id パラメータが指定されていない場合は、すべての DHCP Snooping テーブルエントリ情報が表示されます。

例

#DHCP Snooping テーブルエントリのサマリー情報を表示します。

```
<Sysname> display dhcp snooping binding
2 DHCP snooping entries found
IP address      MAC address     Lease       VLAN  SVLAN Interface
=============== ============== ============ ===== ===== =================
1.1.1.7         0000-0101-0107 16907533     2     3     GE1/0/1
1.1.1.11        0000-0101-010b 16907537     2     3     GE1/0/3
```

#DHCP Snooping テーブルエントリの詳細を表示します。

```
<Sysname> display dhcp snooping binding verbose
IP address: 1.1.1.7
MAC address: 0000-0101-0107
Lease: 16907553 seconds
VLAN: 2
SVLAN: 3
Interface: GigabitEthernet1/0/1
```

Parameter request list: 03 06 21
Client identifier: aabb-aabb-aab1
Authorized client identifier: ccdd-eeff

IP address: 1.1.1.104
MAC address: 0000-0101-010b
Lease: 16907537 seconds
VLAN: 2
SVLAN: 3
Interface: GigabitEthernet1/0/3
Parameter request list: 37 0B 01 0F 03 06 2C 2E 2F 1F 21 F9 2B
Client identifier: aabb-aabb-aab2
Authorized client identifier: aabb-aabb-aab2

表 17-1 display dhcp snooping binding コマンドの表示情報の説明

フィールド	説明
DHCP snooping entries found	テーブル・アイテムの統計数
IP address	DHCPサーバがDHCPクライアントに割り当てるIPアドレス
MAC address	DHCPクライアントのMACアドレス
Lease	バインドされているリースの残り時間 (秒)
VLAN	受信したDHCPメッセージが2つのレイヤVLAN Tagを持つ場合は、外側のレイヤVLAN Tag;それ以外の場合は、DHCPクライアントに接続されているデバイスポートが属するVLANを表します。
SVLAN	受信したDHCPメッセージに2つのレイヤVLAN Tagが含まれている場合は、内側のレイヤVLAN Tag;それ以外の場合は、「N/A」と表示されます。
Interface	DHCPクライアントに接続されているデバイスポート
Parameter request list	DHCPクライアントの要求パラメータ、16進文字列
Client identifier	クライアントID
Authorized client identifier	認証クライアントID

関連コマンド

- **dhcp snooping enable**
- **reset dhcp snooping binding**

17.1.9 display dhcp snooping information

Syntax

display dhcp snooping information { **all** | **interface** *interface-type interface-number* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべてのレイヤ 2 イーサネットインターフェイスに対応する Option 82 設定情報を表示します。

interface *interface-type interface-number*:指定したインタフェースに対応する Option 82 設定情報を表示します。interface-type interface-number はインターフェイスタイプおよびインタフェース番号です。

説明

display dhcp snooping information コマンドは、DHCP Snooping の Option 82 の構成情報を表示するために使用します。

例

#すべてのインタフェースに対応する Option 82 設定情報を表示します。

<Sysname> display dhcp snooping information all

```
Interface: Bridge-Aggregation1
    Status: Disable
    Strategy: Drop
    Circuit ID:
      Padding format: User Defined
        User defined: abcd
      Format: ASCII
    Remote ID:
      Padding format: Normal
      Format: ASCII
    Vendor-specific:
      Padding format: BAS
      Node identifier: MAC
    VLAN 10:
      Circuit ID: abcd
      Remote ID: company
      Vendor-specific:
        Padding format: BAS
        Node identifier: User defined(abcd)
```

表 17-2 display dhcp snooping information コマンドの表示情報の説明

フィールド	説明
Interface	インタフェース名
Status	Option 82のステータス。値はEnableまたはDisableです。
Strategy	Option 82を含むリクエストメッセージの処理ポリシー。値はDrop、Keep、またはReplaceです。
Circuit ID	Circuit IDサブオプションの内容
Padding format	Option 82の塗りつぶしモード: • Circuit ID サブオプションを設定する場合は、Normal、User Defined、Verbose (sysname)、Verbose (MAC)、Verbose (user defined)のいずれかの値を指定します。 • Remote ID サブオプションを設定する場合は、Normal、Sysname、User Defined のいずれかの値を指定します。 • Vendor-specific サブオプションを設定すると、BAS に値が設定されます。
Node identifier	アクセスノードの識別 • Circuit ID、Remote ID サブオプションの入力時にカスタム文字列として値を取得する • Vendor-specific サブオプションを入力すると、MAC、Sysname、User Defined (string)のいずれかの値がカッコ内にカスタム文字列として入力されます。
User defined	ユーザ定義のサブオプションの内容
Format	Option 82サブオプションの塗りフォーマット • Circuit ID サブオプションを設定する場合は、ASCII、Default、または Hex の値を指定します。 • Remote ID サブオプションを設定する場合は、ASCII または Hex の値を指定します。
Remote ID	Remote IDサブオプションの内容
Vendor-specific	Vendor-specificサブオプションの内容は、設定されている場合にのみ表示されます。
VLAN	指定されたVLAN内で受信されたDHCPメッセージには、Circuit IDサブオプション、Remote IDサブオプション、およびVendor-specificサブオプションの内容が設定されます。

17.1.10 display dhcp snooping packet statistics

Syntax

display dhcp snooping packet statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display dhcp snooping packet statistics コマンドは、DHCP Snooping デバイスの DHCP メッセージ統計情報を表示するために使用します。

例

#DHCP Snooping デバイスの DHCP メッセージ統計情報を表示します。

<Sysname> display dhcp snooping packet statistics

DHCP packets received ：100

DHCP packets sent ：200

Invalid DHCP packets dropped ：0

表 17-3 display dhcp snooping packet statistics コマンドの表示情報の説明

フィールド	説明
DHCP packets received	受信したDHCPメッセージの数
DHCP packets sent	送信されたDHCPメッセージの数
Invalid DHCP packets dropped	ドロップされた無効なDHCPメッセージの数

関連コマンド

- **reset dhcp snooping packet statistics**

17.1.11 display dhcp snooping trust

Syntax

display dhcp snooping trust

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display dhcp snooping trust コマンドを使用して、信頼ポート情報を表示します。

例

#信頼ポート情報を表示します。

<Sysname> display dhcp snooping trust

DHCP snooping is enabled.

Interface	Trusted	VLAN
GigabitEthernet1/0/1	Trusted	-
GigabitEthernet1/0/2	-	100
GigabitEthernet1/0/3	-	100, 200

VSI(Trust tunnel)	Trusted
a	Trusted

Interface	SrvID	Trusted
GigabitEthernet1/0/1	1	Trusted

表 17-4 display dhcp snooping trust コマンドの表示情報の説明

フィールド	説明
DHCP snooping is	DHCP Snoopingは、次の値を使用してオンになっています。 • enable:DHCP Snooping 機能を有効にする • disable:DHCP Snooping 機能が有効になっていません
Interface	インタフェース名
VSI (Trust tunnel)	トンネルインターフェイスのVSI名。VSI viewでdhcp snooping trust tunnelコマンドを設定すると表示されます。
SrvID	信頼インタフェースのイーサネットサービスインスタンス番号
Trusted	グローバルDHCP Snooping機能で設定された信頼インタフェース。VLAN内DHCP Snooping機能で構成された信頼インタフェースの場合、ここでは 「-」 と表示されます。
VLAN	信頼ポートが属するVLAN。グローバルDHCP Snooping機能で構成された信頼インタフェースの場合、ここでは 「-」 と表示されます。

関連コマンド

- **dhcp snooping trust**

- **dhcp snooping trust interface**

17.1.12 reset dhcp snooping binding

Syntax

reset dhcp snooping binding { **all** | **ip** *ip-address* [**vlan** *vlan-id*] }

View

User view

定義済みユーザロール

network-admin

パラメータ

all:すべての DHCP Snooping テーブルエントリを消去します。

ip *ip-address*:指定した IP アドレスの DHCP Snooping テーブルエントリをクリアします。

vlan *vlan-id*:指定した VLAN 内の DHCP Snooping テーブルエントリをクリアします。このパラメータが指定されていない場合、デフォルト VLAN 内の DHCP Snooping テーブルエントリはクリアされます。

説明

reset dhcp snooping binding コマンドは、DHCP Snooping テーブルエントリをクリアするために使用します。

例

#すべての DHCP Snooping テーブルエントリをクリアします。

<Sysname> reset dhcp snooping binding all

関連コマンド

- **display dhcp snooping binding**

17.1.13 reset dhcp snooping packet statistics

Syntax

reset dhcp snooping packet statistics

View

User view

定義済みユーザロール

network-admin

説明

reset dhcp snooping packet statistics コマンドは、DHCP Snooping デバイスの DHCP メッセージ統計情報をクリアするために使用します。

例

#DHCP Snooping デバイスの DHCP メッセージ統計情報をクリアします。

<Sysname> reset dhcp snooping packet statistics

関連コマンド

- **display dhcp snooping packet statistics**

目次

このセクションのページは **5-x-x** です。

18 章 DNS 18-1
18.1 DNS 設定コマンド 18-1
18.1.1 display dns domain 18-1
18.1.2 display dns host 18-2
18.1.3 display dns server 18-3
18.1.4 dns domain 18-5
18.1.5 dns dscp 18-6
18.1.6 dns proxy enable 18-6
18.1.7 dns server 18-7
18.1.8 ip host 18-8
18.1.9 reset dns host 18-9

18章 DNS

18.1 DNS設定コマンド

18.1.1 display dns domain

Syntax

display dns domain [**dynamic**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic : DHCP などのプロトコルで動的に取得されたドメイン名サフィックス情報を表示する。このパラメータが指定されていない場合は、静的に構成され、動的に取得されたドメイン名サフィックス情報が表示されます。

説明

display dns domain コマンドは、ドメイン名サフィックス情報を表示するために使用します。

例

#パブリックネットワークの静的設定および動的に取得されたドメイン名サフィックス情報を表示します。

<Sysname> display dns domain
Type:
D: Dynamic S: Static

No. Type Domain suffix
1 S com
2 D net

表 18-1 display dns domain コマンドの表示情報の説明

フィールド	説明
No.	連番

フィールド	説明
Type	ドメイン名サフィックスのタイプ: • S:静的構成を表すドメイン名サフィックス • D:DHCP などのプロトコルで動的に獲得されたドメイン名を表す接尾辞
Domain suffix	ドメインサフィックス

関連コマンド

- **dns domain**

18.1.2 display dns host

Syntax

display dns host [**ip**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip:クラス A クエリの情報を表示します。クラス A クエリは、ドメイン名に対応する IPv4 アドレスを解決するために使用されます。

説明

display dns host コマンドを使用して、ドメイン名解決情報を表示します。

ip パラメータが指定されていない場合は、すべてのクエリタイプのドメイン名解決情報が表示されます。

例

#パブリックネットワークのすべてのクエリタイプの静的ドメイン名解決テーブルと動的ドメイン名解決キャッシュテーブルのドメイン名解決情報を表示します。

<Sysname> display dns host

Type:

D: Dynamic S: Static

Total number: 4

No. Host name Type TTL Query type IP addresses

```
1    sample.com          D   3132        A      192.168.10.1
                                                192.168.10.2
                                                192.168.10.3
2    sample1.com         D   2400(a)     A      100.10.23.1
3    zig.sample.com      S   -           A      192.168.1.1
4    sample.net          S   -           AAAA   FE80::4904:4448
```

表 18-2 display dns host コマンドの表示情報の説明

フィールド	説明
No.	連番
Host name	クエリのドメイン名
Type	ドメイン名解決情報のタイプ: • S:静的に構成されたドメイン名解決情報、つまり ip host または ipv6 host コマンドで構成されたホスト名とそれに対応するホスト IPv4/IPv6 アドレス • D:動的ドメイン名解決によって得られたドメイン名解決情報を表す.
TTL	ドメイン名解決情報の残りの有効時間 (秒) (a) は、テーブルエントリのエージング時間がdns domain aging-timeコマンドで指定され、このコマンドで指定されたドメインテーブルエントリが永続的に有効な場合はInfiniteと表示されることを示します。 静的ドメイン名解決情報の場合、このフィールドは 「-」と表示されます。
Query type	AおよびAAAAを含む値を取得する問合せタイプ
IP addresses	ホスト名に対応するIPアドレス • タイプ A クエリの場合は IPv4 アドレス • AAAA クラス照会タイプの場合は IPv6 アドレス

関連コマンド

- **reset dns host**
- **ip host**

18.1.3 display dns server

Syntax

display dns server [**dynamic**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic:DHCP などのプロトコルで動的に取得されたドメインネームサーバ IPv 4 アドレス情報を表示する。このパラメータを指定しない場合は、静的に構成され、動的に取得されたドメインネームサーバの IPv 4 アドレス情報が表示されます。

説明

display dns server コマンドは、ドメインネームサーバの IPv 4 アドレス情報を表示します。

例

#パブリックネットワークのドメインネームサーバ IPv 4 アドレス情報を表示します。

<Sysname> display dns server

Type:

D: Dynamic S: Static

No. Type IP address

1 S 202.114.0.124

2 S 169.254.65.125

表 18-3 display dns server コマンドの表示情報の説明

フィールド	説明
No.	ドメインネームサーバのシーケンス番号
Type	ドメインネームサーバのタイプ • S は静的に指定されたドメインネームサーバ情報を表す. • D は DHCP などのプロトコルで動的に得られるドメインネームサーバ情報を表す.
IP address	ドメインネームサーバのIPv 4アドレス

関連コマンド

- **dns server**

関連コマンド

18.1.4 dns domain

Syntax

dns domain *domain-name*

undo dns domain *domain-name*

デフォルト

ドメイン名サフィックスが設定されていません。つまり、ユーザが入力したドメイン名情報のみに基づいて解決されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: 「.」 で区切られた文字列で構成されるドメイン名サフィックス(例 aabbcc.com)。各文字列の長さは 63 文字以内で、 「.」 を含めた全体の長さは 253 文字以内です。大文字と小文字は区別されず、文字列には文字、数字、 「-」 、 「_」 、または 「.」 を含めることができます。

説明

dns domain コマンドは、ドメイン名サフィックスを追加するために使用します。

undo dns domain コマンドは、指定されたドメイン名サフィックスを削除します。

ドメイン名を解決する時、ユーザはドメイン名の一部のフィールドを入力するだけでよく、システムはドメイン名のサフィックス配置の先着順に従い、順次に入力したドメイン名に異なるドメイン名サフィックスを加えて解決する。

このコマンドで設定されるドメイン名サフィックスは、IPv4 ドメイン名解決に使用されます。

パブリックネットワークには、最大 16 個のドメイン名サフィックスを設定できます。

例

#パブリックネットワークのドメイン名サフィックス com を追加します。

<Sysname> system-view
[Sysname] dns domain com

関連コマンド

- **display dns domain**

18.1.5 dns dscp

Syntax

dns dscp *dscp-value*

undo dns dscp

デフォルト

DNS クライアントまたは DNS proxy が DNS メッセージを送信する DSCP の優先順位は 0 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value:DNS メッセージの DSCP 優先度。範囲は 0~63 です。

説明

dns dscp コマンドは、DNS クライアントまたは DNS proxy が DNS メッセージを送信する DSCP の優先順位を指定するために使用します。

undo dns dscp コマンドを使用して、デフォルトの状態を復元します。

DSCP 優先度は、メッセージ自体の優先度を表し、メッセージ転送の優先度を決定する。DSCP 優先度の設定値が大きいほど、メッセージの優先度が高くなります。

例

#送信される DNS メッセージの DSCP 優先順位を 30 に設定します。

<Sysname> system-view
[Sysname] dns dscp 30

18.1.6 dns proxy enable

Syntax

dns proxy enable

undo dns proxy enable

デフォルト

DNS proxy 機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

dns proxy enable コマンドは、DNS proxy 機能を有効にするために使用します。

undo dns proxy enable コマンドは、DNS proxy 機能をオフにするために使用します。

このコマンドの設定は、IPv4 ドメイン名解決に使用されます。

例

#DNS proxy を有効にします。

<Sysname> system-view
[Sysname] dns proxy enable

18.1.7 dns server

Syntax

dns server *ip-address*

undo dns server [*ip-address*]

デフォルト

ドメインネームサーバの IPv 4 アドレスが構成されていません。

View

System view

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address:ドメインネームサーバの IPv 4 アドレス。このパラメータは、Interface view で undo コマンドを実行するときに指定します。

説明

dns server コマンドは、ドメインネームサーバの IPv 4 アドレスを設定します。

undo dns server コマンドは、ドメインネームサーバの IPv 4 アドレスを削除します。

動的なドメイン名解決を行う場合、システムはドメインネームサーバの IPv 4 アドレス配置の先着順に各ドメインネームサーバに問合せ要求を送信する。

パブリックネットワークには、最大 6 つのドメインネームサーバの IPv 4 アドレスを設定できます。

undo dns server コマンドの実行時に ip-address パラメータが指定されていない場合は、パブリックネットワーク内のすべてのドメインネームサーバ IPv 4 アドレスが削除されます。

例

#ドメインネームサーバの IPv 4 アドレスを 172.16.1.1 に設定します。

<Sysname> system-view
[Sysname] dns server 172.16.1.1

#VLAN インタフェース 2 のドメインネームサーバの IPv 4 アドレスを 172.16.1.1 に設定します。

<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] dns server 172.16.1.1

関連コマンド

- **display dns server**

18.1.8 ip host

Syntax

ip host *host-name ip-address*

undo ip host *host-name ip-address*

デフォルト

ホスト名と IPv 4 アドレスの対応関係は存在しない。

View

System view

定義済みユーザロール

network-admin

パラメータ

host-name:ホスト名。大文字と小文字を区別しない 1~253 文字の文字列で、文字、数字、「-」 、 「_」 、 「.」 を使用できます。

ip-address:ホスト名に対応する IPv 4 アドレス。

説明

ip host コマンドは、ホスト名とそれに対応するホスト IPv 4 アドレスを構成します。

undo ip host コマンドは、ホスト名とそれに対応するホスト IPv 4 アドレスを削除します。

パブリックネットワークでは、最大 1024 個のホスト名と IPv 4 アドレスの対応を構成できます。

パブリックネットワークでは、1 つのホスト名に対応できる IPv 4 アドレスは 1 つだけです。このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

ip、-a、-c、-f、-h、-i、-m、-n、-p、-q、-r、-s、-t、-tos、-v、-vpn-instance は、ping コマンドの引数キーワードとして使用されています。ホスト名を設定する場合は、同じ文字列をホスト名として使用しないでください。ping コマンドでサポートされているパラメータの形式については、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*17 ネットワーク管理と監視*”の”*1 章 システムの保守*”を参照してください。

例

#パブリックネットワーク内のホスト名 aaa に対応する IPv 4 アドレスを 10.110.0.1 に設定します。

<Sysname> system-view
[Sysname] ip host aaa 10.110.0.1

関連コマンド

- **display dns host**

18.1.9 reset dns host

Syntax

reset dns host [**ip**]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip:クラス A クエリの動的キャッシュ情報をクリアします。クラス A クエリは、ドメイン名に対応する IPv4 アドレスを解決するために使用されます。

説明

reset dns host コマンドは、動的ドメイン名解決キャッシュ情報をクリアするために使用します。

ip パラメータが指定されていない場合は、すべてのクエリタイプの動的ドメイン名解決キャッシュ情報がクリアされます。

例

#パブリックネットワークのすべてのクエリタイプの動的ドメイン名解決キャッシュ情報をクリアします。

<Sysname> reset dns host

関連コマンド

- **display dns host**

目次

このセクションのページは **5-x-x** です。

19 章 HTTP 19-1
19.1 HTTP 設定コマンド 19-1
19.1.1 display ip http 19-1
19.1.2 display ip https 19-2
19.1.3 ip http acl 19-3
19.1.4 ip http enable 19-4
19.1.5 ip http port 19-5
19.1.6 ip https acl 19-5
19.1.7 ip https enable 19-7
19.1.8 ip https port 19-8
19.2 HTTP リダイレクト設定コマンド 19-8
19.2.1 http-redirect https-rate-limit 19-8

19章 HTTP

19.1 HTTP設定コマンド

19.1.1 display ip http

Syntax

display ip http

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip http コマンドは、HTTP のステータス情報を表示するために使用します。

例

#HTTP のステータス情報を表示します。

<Sysname> display ip http

HTTP port:80

Basic ACL:2222

HTTP status:Enabled

表 19-1 display ip http コマンドの表示情報の説明

フィールド	説明
HTTP port	HTTPサービスが使用するポート番号
Basic ACL	HTTPサービスに関連付けられている基本アクセス制御リスト番号または名前。0は未構成
HTTP status	HTTPサービスがオンになっているかどうか: Enabled:HTTPサービスがオンであることを示します。 Disabled:HTTPサービスが停止していることを示します。

関連コマンド

- **ip http port**
- **ip http acl**

- **ip http enable**

19.1.2 display ip https

Syntax

display ip https

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip https コマンドは、HTTPS のステータス情報を表示するために使用します。

例

#HTTPS のステータス情報を表示します。

<Sysname> display ip https

HTTPS port:443

SSL server policy:test

Certificate access control policy:Not configured

Basic ACL:2222

HTTPS status:Enabled

表 19-2 display ip https コマンドの表示情報の説明

フィールド	説明
HTTPS port	HTTPSサービスが使用するポート番号
SSL server policy	HTTPSサービスに関連付けられたSSLサーバー側ポリシー。Not configuredは構成されていないことを示します。
Certificate access-control-policy	HTTPSサービスに関連付けられた証明書属性アクセスコントロールポリシー、Not configuredは設定されていないことを示します
Basic ACL	HTTPSサービスに関連付けられた基本アクセス制御リスト番号または名前。0は未構成
HTTPS status	HTTPSサービスがオンになっているかどうか Enabled:HTTPSサービスがオンであることを示します。 Disabled:HTTPSサービスが停止していることを示します。

関連コマンド

- **ip https port**
- **ip https acl**
- **ip https enable**
- **ip https ssl-server-policy**
- **ip https certificate access-control-policy**

19.1.3 ip http acl

Syntax

ip http acl { *acl-number* | **name** *acl-name* }

undo ip http acl

デフォルト

HTTP サービスは ACL に関連付けられていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number:ACL の番号。範囲は 2000~2999 (基本 IPv4 ACL)です。

name *acl-name*:ACL の名前を指定します。acl-name は、ACL の名前を表す 1~63 文字の文字列です。大文字と小文字は区別されず、a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。指定された名前の ACL が存在し、ベース IPv4 ACL である場合にのみ有効です。

説明

ip http acl コマンドは、ACL に関連付けられた HTTP サービスを設定するために使用します。

undo ip http acl コマンドを使用して、デフォルトの状態を復元します。

このコマンドを複数回実行すると、最新の設定が有効になります。

HTTP サービスを ACL に関連付けるように設定すると、ACL で許可されている HTTP クライアントだけが Web 経由でデバイスにログインできます。一致しない ACL または ACL によって拒否された HTTP クライアントは、Web 経由でデバイスにログインできません。

例

#ACL 2001 に関連付けられた HTTP サービスを設定し、10.10.0.0/16 セグメントのクライアントのみが Web 経由でデバイスにアクセスできるようにします。

<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip http acl 2001

関連コマンド

- **acl (セキュリティ/ACL)**

19.1.4 ip http enable

Syntax

ip http enable

undo ip http enable

デフォルト

HTTP サービスが停止しています。

View

System view

定義済みユーザロール

network-admin

説明

ip http enable コマンドは、HTTP サービスを開始するために使用します。

undo ip http enable コマンドは、HTTP サービスを停止するために使用します。

HTTP サービスを有効にすると、ユーザは Web 経由で HTTP を使用してデバイスにログインできます。

HTTP サービスを有効にすると、デバイスのセキュリティを強化するために、HTTPS サービスのポート番号も自動的に有効になり、HTTP サービスが有効になっている間は **undo ip https enable** コマンドで無効にできません。

例

#HTTP サービスを有効にする。

<Sysname> system-view
[Sysname] ip http enable

関連コマンド

- **ip https enable**

19.1.5 ip http port

Syntax

ip http port *port-number*

undo ip http port

デフォルト

HTTP サービスのポート番号は 80 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number:HTTP サービスのポート番号。範囲は 1~65535 です。

説明

ip http port コマンド HTTP サービスを構成するために使用するポート番号。

undo ip http port コマンドを使用して、デフォルトの状態を復元します。

ポート番号を変更する前に HTTP サービスがオンになっていた場合、ポート番号を変更すると HTTP サービスが自動的に再起動され、アクセス中のユーザは切断されます。ユーザがアクセスを続行するには、ブラウザのアドレスバーに新しいアドレスを再入力する必要があります。

例

#HTTP サービスのポート番号を 80 に設定します。

<Sysname> system-view
[Sysname] ip http port 80

19.1.6 ip https acl

Syntax

ip https acl {*acl-number* | **name** *acl-name*}

undo ip https acl

デフォルト

HTTPS サービスは ACL に関連付けられていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number:ACL の番号。範囲は 2000~2999 (基本 IPv4 ACL)です。

name *acl-name*:ACL の名前を指定します。acl-name は、ACL の名前を表す 1~63 文字の文字列です。大文字と小文字は区別されず、a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。指定された名前の ACL が存在し、ベース IPv4 ACL である場合にのみ有効です。

説明

ip https acl コマンドは、ACL に関連付けられた HTTPS サービスを設定するために使用します。

undo ip https acl コマンドを使用して、デフォルトの状態を復元します。

HTTPS サービスを ACL に関連付けるように設定すると、ACL で許可されている HTTPS クライアントだけが Web 経由でデバイスにログインできます。一致しない ACL または ACL によって拒否された HTTPS クライアントは、Web 経由でデバイスにログインできません。

なお、 Web ログイン時にユーザが入力するユーザ名とパスワードは機密情報であり、Web ログイン要求は HTTPS 方式で Web サーバに送信される。したがって、このコマンドの ACL ルールでクライアントが HTTPS サービスを介して Web ページにアクセスすることを拒否した場合、クライアントは HTTP サービスを介して Web ページにアクセスすることもできません。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

#設定 HTTPS サービスは ACL 2001 に関連付けられ、10.10.0.0/16 セグメントのクライアントだけが Web 経由でデバイスにアクセスできるようにします。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ip https acl 2001
```

関連コマンド

- **acl (セキュリティ/ACL)**

19.1.7 ip https enable

Syntax

ip https enable

undo ip https enable

デフォルト

HTTPS サービスが停止しています。

View

System view

定義済みユーザロール

network-admin

説明

ip https enable コマンドは、HTTPS サービスを開始するために使用します。

undo ip https enable コマンドは、HTTPS サービスを停止するために使用します。

この機能を有効にするまで、ユーザは HTTPS を使用して Web からデバイスにログインできません。

HTTPS サービスを有効にすると、SSL ハンドシェイクネゴシエーションプロセスがトリガーされます。SSL ハンドシェークネゴシエーション中に、デバイスのローカル証明書がすでに存在する場合、SSL ネゴシエーションは成功し、HTTPS サービスは正常に開始されます。アプライアンスのローカル証明書が存在しない場合、SSL ネゴシエーションプロセスによって証明書要求プロセスがトリガーされます。証明書の申請に時間がかかるため、SSL ネゴシエーションが失敗し、HTTPS サービスが正常に開始されません。したがって、この場合、ip https enable サービスが正常に起動するには、HTTPS コマンドを複数回実行する必要があります。

例

#HTTPS サービスを有効にします。

<Sysname> system-view
[Sysname] ip https enable

関連コマンド

- **ip https ssl-server-policy**
- **ip https certificate access-control-policy**

19.1.8 ip https port

Syntax

ip https port *port-number*

undo ip https port

デフォルト

HTTPS サービスのポート番号は 443 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number:HTTPS サービスのポート番号。範囲は 1~65535 です。

説明

ip https port コマンド HTTPS サービスを設定するために使用されるポート番号。

undo ip https port コマンドを使用して、デフォルトの状態を復元します。

ポート番号を変更する前に HTTPS サービスがオンになっていた場合、ポート番号を変更すると HTTPS サービスは自動的に再起動され、アクセス中のユーザは接続解除されます。ユーザがアクセスを続行するには、ブラウザのアドレスバーに新しいアドレスを再入力する必要があります。

例

#設定 HTTPS サービスのポート番号は 8080 です。

<Sysname> system-view
[Sysname] ip https port 8080

19.2 HTTPリダイレクト設定コマンド

19.2.1 http-redirect https-rate-limit

メモ:

本コマンドはソフトウェアバージョン 9.4.13 を含む以降のソフトウェアからサポートしています。9.4.09 以前のソフトウェアはレート制限がありません。

Syntax

http-redirect https-rate-limit *pps*

undo http-redirect https-rate-limit

デフォルト

Ver9.4.13 以降：100

Ver9.4.09 以前：制限なし

View

System view

定義済みユーザロール

network-admin

パラメータ

pps: HTTP リダイレクトパケットのレート制限。範囲は 1~65535 です。

説明

http-redirect https-rate-limit コマンドを使用して HTTPS リダイレクトパケットのレートを設定します。

undo http-redirect https-rate-limit コマンドは、設定をデフォルトに戻します。

例

HTTP リダイレクトパケットのレートを 50pps に設定する。

<Sysname> system-view
[Sysname] http-redirect https-rate-limit 50

目次

このセクションのページは **5-x-x** です。

20 章 IP パフォーマンスの最適化 20-1
20.1 IP パフォーマンスの最適化設定コマンド 20-1
20.1.1 display icmp statistics 20-1
20.1.2 display ip statistics 20-2
20.1.3 display rawip 20-4
20.1.4 display rawip verbose 20-5
20.1.5 display tcp 20-9
20.1.6 display tcp verbose 20-11
20.1.7 display udp 20-16
20.1.8 display udp statistics 20-17
20.1.9 display udp verbose 20-18
20.1.10 ip forward-broadcast 20-23
20.1.11 ip icmp error-interval 20-24
20.1.12 ip mtu 20-25
20.1.13 ip redirects enable 20-26
20.1.14 ip ttl-expires enable 20-27
20.1.15 ip unreachables enable 20-28
20.1.16 reset ip statistics 20-29
20.1.17 reset udp statistics 20-29
20.1.18 tcp path-mtu-discovery 20-30
20.1.19 tcp timer fin-timeout 20-31
20.1.20 tcp timer syn-timeout 20-32
20.1.21 tcp window 20-33

20章 IP パフォーマンスの最適化

20.1 IPパフォーマンスの最適化設定コマンド

20.1.1 display icmp statistics

Syntax

display icmp statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display icmp statistics コマンドを使用して、ICMP トラフィック統計情報を表示します。

display icmp statistics コマンドは、デバイスが送受信するさまざまな ICMP トラフィックの統計情報を表示します。

例

#ICMP トラフィックの統計情報を表示します。

<Sysname> display icmp statistics

```
  Input: bad formats     0                    bad checksum                0
         echo            175                  destination unreachable 0
         source quench 0                      redirects                   0
         echo replies    201                  parameter problem           0
         timestamp       0                     information requests       0
         mask requests 0                      mask replies                0
         time exceeded 0                      invalid type                0
         router advert 0                     router solicit          0
         broadcast/multicast echo requests ignored          0
         broadcast/multicast timestamp requests ignored     0
 Output: echo            0                    destination unreachable 0
         source quench 0                      redirects                   0
         echo replies    175                  parameter problem           0
         timestamp       0                     information replies        0
         mask requests 0                      mask replies                0
         time exceeded 0                      bad address                 0
```

packet error　1442　　router advert　　3

表 20-1 display icmp statistics コマンドの表示情報の説明

フィールド	説明
bad formats	入力されたフォーマット・エラー・メッセージの数
bad checksum	入力されたチェックサムエラーメッセージの数
echo	入出力応答要求メッセージ数
destination unreachable	入出力の目的到達不能メッセージ数
source quench	入出力の発信元抑制メッセージ数
redirects	入出力リダイレクトメッセージの数
echo replies	入出力応答メッセージ数
parameter problem	入出力のパラメータエラーメッセージ数
timestamp	入力されたタイムスタンプ要求メッセージ数/出力されたタイムスタンプ応答メッセージ数
information requests	入力された情報要求メッセージの数
mask requests	入出力マスク要求メッセージ数
mask replies	入出力マスク応答メッセージ数
invalid type	入力された不正なタイプのメッセージ数
router solicit	入力されたルータ要求メッセージ数
broadcast/multicast echo requests ignored	入力されたブロードキャスト/マルチキャスト応答要求ドロップメッセージの数
broadcast/multicast timestamp requests ignored	入力されたブロードキャスト/マルチキャストタイムスタンプリクエスト廃棄メッセージ数
information replies	出力するメッセージ応答メッセージ数
time exceeded	入出力のタイムアウトメッセージ数
bad address	出力された宛先アドレスの不正メッセージ数
packet error	出力されたエラーメッセージ数
router advert	入出力ルータアナウンスメッセージ数

20.1.2 display ip statistics

Syntax

display ip statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip statistics コマンドを使用して、IP メッセージの統計情報を表示します。

display ip statistics コマンドを使用して、受信メッセージ、送信メッセージ、シャード、再編成などの IP メッセージ統計を表示します。

例

#IP メッセージの統計情報を表示します。

<Sysname> display ip statistics

```
Input:          sum              7120          local            112
                bad protocol     0             bad format       0
                bad checksum     0             bad options      0
                dropped          0
Output:         forwarding       0             local            27
                dropped          0             no route         2
                compress fails 0
Reassembling:   fragments        0             reassembled      0
                dropped          0             timeouts         0
Fragment:       fragmented       0             couldn't fragment 0
                output frags     0
Forwarded Frags: sum             0
```

表 20-2 display ip statistics コマンドの表示情報の説明

フィールド		説明
Input:	sum	受信メッセージ総数
	local	受信した宛先アドレスはローカルメッセージ数である.
	bad protocol	不明なプロトコルのメッセージ数
	bad format	フォーマットエラーのメッセージ数
	bad checksum	チェックサムエラーのメッセージ数
	bad options	オプションエラーのメッセージ数
	dropped	受信時に破棄されたメッセージ数
Output:	forwarding	転送されたメッセージ数
	local	ローカル送信メッセージ数
	dropped	送信時に破棄されたメッセージ数
	no route	ルートが検出されなかったメッセージ数
	compress fails	圧縮に失敗したメッセージ数
Reassembling:	fragments	再編成が必要なシャードメッセージの受信数
	reassembled	再編成に成功したメッセージ数
	dropped	再編成に失敗した後に廃棄されたシャードメッセージの数
	timeouts	再編成タイムアウトの回数

フィールド		説明
Fragment:	fragmented	シャードに成功したメッセージ数
	couldn't fragment	シャードに失敗したメッセージ数
	output frags	シャードが成功し、送信されたシャードメッセージの数
Forwarded Frags:	sum	直接転送されたシャードメッセージの数

関連コマンド

- **display ip interface (ネットワーク接続/IP アドレス)**
- **reset ip statistics**

20.1.3 display rawip

Syntax

display rawip

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display rawip コマンドは、RawIP 接続サマリー情報を表示するために使用します。

display rawip コマンドを使用すると、ローカル IP アドレス、ピア IP アドレス、RawIP socket を使用するプロトコル番号などの情報を含む RawIP 接続サマリー情報を表示できます。

例

#RawIP 接続サマリー情報を表示します。

<Sysname> display rawip

#: Kernel RawIP connection

Local Addr	Foreign Addr	Protocol	PCB
0.0.0.0	0.0.0.0	1	0x0000000000000009
0.0.0.0	0.0.0.0	1	0x0000000000000008
0.0.0.0	0.0.0.0	1	0x0000000000000002
#0.0.0.0	0.0.0.0	1	N/A

表 20-3　display rawip コマンドの表示情報の説明

フィールド	説明
#	接続の前にこのIDが表示されている場合は、RawIP接続がComwareカーネルによって使用されている接続であることを示します。
Local Addr	ローカルIPアドレス
Foreign Addr	ピアIPアドレス
Protocol	RawIP socketのプロトコル番号を使用
PCB	プロトコル制御ブロックインデックス

20.1.4 display rawip verbose

Syntax

display rawip verbose [**pcb** *pcb-index*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display rawip verbose コマンドは、RawIP 接続の詳細を表示するために使用します。

display rawip verbose コマンドを使用すると、socket の作成者、ステータス、オプション、タイプ、使用されているプロトコル番号、RawIP 接続の送信元 IP アドレスと宛先 IP アドレスなどの情報を含む、RawIP 接続の詳細を表示できます。

例

#RawIP 接続の詳細を表示します。

<Sysname> display rawip verbose

Total RawIP socket number: 1

Connection info: src = 0.0.0.0, dst = 0.0.0.0

Creator: ping[320]

State: N/A

Options: N/A

Error: 0

Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A

Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A

Type: 3

Protocol: 1

Inpcb flags: N/A

Inpcb extflag: INP_EXTRCVICMPERR INP_EXTFILTER

Inpcb vflag: INP_IPV4

TTL: 255(minimum TTL: 0)

Sending VRF: 0x0

Receiving VRF: 0x0

表 20-4　display rawip verbose コマンドの表示情報の説明

フィールド	説明
Total RawIP socket number	RawIP socket合計
Connection info	接続情報:送信元IPアドレス、宛先IPアドレス
Creator	socketを作成したタスクの名前。カッコ内は作成者のプロセス番号
State	socketのステータス。次を含みます。 • NOFDREF:ユーザが終了しました • ISCONNECTED:接続が確立されました • ISCONNECTING:接続を確立中 • ISDISCONNECTING:切断中 • ISDISCONNECTED:接続が切断されました • ISPCBSYNCING:internetプロトコル制御ブロックを同期中 • ISSMOOTHING:スムージング • N/A:上記の状態ではありません

フィールド	説明
Options	socketのオプション: • SO_DEBUG:ソケットのデバッグ情報を記録します。 • SO_ACCEPTCONN:serverエンドリスニング接続リクエスト • SO_REUSEADDR:ローカルアドレスの再使用を許可する • SO_KEEPALIVE:プロトコルはアイドル状態の接続を問い合わせる必要があります • SO_DONTROUTE:ルーティングテーブルを調べないように設定する(宛先アドレスが直接接続ネットワークの場合に用いる.) • SO_BROADCAST:ソケットサポートブロードキャストメッセージ • SO_LINGER:ソケットは閉じられているが、まだ残りのデータを送信している • SO_OOBINLINE:帯域外データをインラインで保存 • SO_REUSEPORT:ローカル・ポートの再使用を許可 • SO_TIMESTAMP:接続されていないプロトコルでのみ有効な入力メッセージのタイムスタンプをミリ秒単位で記録します。 • SO_FILTER:受信メッセージに有効なメッセージ・フィルタ条件を設定します。 • SO_TIMESTAMPNS:タイムスタンプオプションと同様に、ナノ秒までの正確な時間 • N/A:オプションが設定されていません
Error	socket接続に影響するエラーコード
Receiving buffer (cc/hiwat/lowat/drop/state)	受信バッファ情報は、現在の使用領域、最大領域、最小領域、ドロップ数、状態でかっこで囲まれます。次の情報が含まれます。 • CANTSENDMORE:データをピアに送信できない • CANTRCVMORE:ピアからデータを受信できない • N/A:上記の状態ではありません
Sending buffer (cc/hiwat/lowat/state)	現在の使用領域、最大領域、最小領域、ステータスをかっこで囲んでバッファ情報を送信します。 • CANTSENDMORE:データをピアに送信できない • CANTRCVMORE:ピアからデータを受信できない • N/A:上記の状態ではありません

フィールド	説明
Type	使用されているsocketタイプは次のとおりです。 ● 1:SOCK_STREAM、ストリームモード、信頼性の高いバイトストリームを提供します。TCPプロトコルはこのタイプを使用します。 ● 2:SOCK_DGRAM、データグラムモードの通信。UDPプロトコルはこのタイプを使用します。 ● 3:SOCK_RAW、RAWモードの通信方式 ● N/A:上記のタイプではありません
Protocol	socketのプロトコル番号を使用
Inpcb flags	Internetプロトコル制御ブロック内のタグ。次のものが含まれます。 ● INP_RECVOPTS:受信IPオプション ● INP_RECVRETOPTS:応答を受信するIPオプション ● INP_RECVDSTADDR:宛先IPアドレスの受信 ● INP_HDRINCL:IPヘッダ全体をユーザが指定します。 ● INP_REUSEADDR:アドレスの再使用 ● INP_REUSEPORT:ポート番号の再使用 ● INP_ANONPORT:ユーザがポートを指定していません ● INP_RECVIF:メッセージ受信時にメッセージを記録するための入力インタフェース ● INP_RECVTTL:メッセージを送信するTTL、UDPとRawIPのみサポート ● INP_DONTFRAG:シャード不可フラグの設定 ● INP_ROUTER_ALERT:ルータ警告オプションを含むメッセージを受信します。RawIPのみサポートされます。 ● INP_PROTOCOL_PACKET:メッセージがプロトコル・メッセージであることを示します。 ● INP_RCVVLANID:受信メッセージのVLAN ID、UDPとRawIPのみサポート ● INP_RCVMACADDR:受信メッセージのMAC ● INP_RECVTOS:メッセージを運ぶTOS、UDPとRawIPのみサポート ● INP_USEICMPSRC:設定されたICMPアドレスを送信元アドレスとして使用します。 ● N/A:上記のタグではありません

フィールド	説明
Inpcb extflag	Internetプロトコル制御ブロック内の拡張タグ。次のものが含まれます。 ● INP_EXTRCVPVCIDX:メッセージ受信時にメッセージを記録するPVCインデックス ● INP_RCVPWID:メッセージ受信時にメッセージを記録するPW ID ● INP_EXTRCVICMPERR:ICMPエラーメッセージを受信します。 ● INP_EXTFILTER:メッセージ受信時にメッセージ内容をフィルタリングする. ● N/A:上記のタグではありません
Inpcb vflag	Internetプロトコル制御ブロックのIPバージョンタグ。次のものが含まれます。 ● INP_IPv 4:IPv 4との通信に使用 ● N/A:上記のタグではありません
TTL (minimum TTL)	Internetプロトコル制御ブロック中の生存期間、括弧内は最小生存期間
Sending VRF	(未サポート)送信インスタンス
Receiving VRF	(未サポート)受入例

20.1.5 display tcp

Syntax

display tcp

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display tcp コマンドは、TCP 接続の概要情報を表示します。

display tcp コマンドは、TCP 接続のサマリー情報を表示します。この情報には、自ポートの IP アドレスとポート番号、ピアの IP アドレスとポート番号、TCP 接続のステータスなどが含まれます。

例

#TCP 接続の概要情報を表示します。

```
<Sysname> display tcp
 *: TCP connection with authentication
 #: Kernel TCP connection
 Local Addr:port        Foreign Addr:port      State        PCB
*0.0.0.0:21             0.0.0.0:0              LISTEN       0x000000000000c387
#1.0.0.1:179            1.0.0.2:29376          ESTABLISHED N/A
 192.168.20.200:23      192.168.20.14:1284     ESTABLISHED 0x0000000000000009
 192.168.20.200:23      192.168.20.14:1283     ESTABLISHED 0x0000000000000002
```

表 20-5　display tcp コマンドの表示情報の説明

フィールド	説明
*	接続の前にこのIDがある場合は、TCP接続が暗号化アルゴリズムを使用して認証された接続であることを示します。
#	接続の前にこのIDが表示されている場合は、TCP接続がComwareカーネルによって使用されている接続であることを示します。
Local Addr:port	ローカルIPアドレスとポート番号
Foreign Addr:port	ピアIPアドレスとポート番号
State	次のTCP接続ステータス。 • CLOSED:クライアントから切断接続要求の応答を受信した後のサーバの状態 • LISTEN:接続要求を待機しているサーバの状態 • SYN_SENT:クライアントが接続要求を発行してサーバからの応答を待っている状態 • SYN_RCVD:サーバがクライアント接続リクエストを受信したときの状態 • ESTABLISHED:サーバとクライアントの両方が接続され、双方向のデータ転送が可能な状態 • CLOSE_WAIT:サーバがクライアントから切断要求を受信したときの状態 • FIN_WAIT_1:クライアントが接続クローズ要求を発行してサーバからの応答を待っている状態 • CLOSING:接続のクローズ要求がピアに発行された後、ピアの応答を待っている間に、接続のクローズ要求がピアから受信されたときの状態 • LAST_ACK:サーバがクライアントにクローズ接続要求を出して応答を待っている状態 • FIN_WAIT_2:クライアントがサーバダウン接続応答を受信した後の状態 • TIME_WAIT:クライアントがサーバから切断接続要求を受信した後の状態
PCB	プロトコル制御ブロックインデックス

20.1.6 display tcp verbose

Syntax

display tcp verbose [**pcb** *pcb-index*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display tcp verbose コマンドを使用して、TCP 接続の詳細を表示します。

display tcp verbose コマンドは、socket の作成者、ステータス、オプション、タイプ、使用されているプロトコル番号、TCP 接続の送信元 IP アドレスとポート番号、宛先 IP アドレスとポート番号、ステータスなどの TCP 接続の詳細を表示します。

例

#TCP 接続の詳細を表示します。

<Sysname> display tcp verbose

TCP inpcb number: 1(tcpcb number: 1)

Connection info: src = 192.168.20.200:179, dst = 192.168.20.14:4181

Creator: bgpd[199]

State: ISCONNECTED

Options: N/A

Error: 0

Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 65700 / 1 / 0 / N/A

Sending buffer(cc/hiwat/lowat/state): 0 / 65700 / 512 / N/A

Type: 1

Protocol: 6

NAT kernel port: 0

Inpcb flags: N/A

Inpcb extflag: N/A

Inpcb vflag: INP_IPV4

TTL: 255(minimum TTL: 0)

Connection state: ESTABLISHED

TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR

NSR state: READY(M)

Sending VRF: 0x0

Receiving VRF: 0x0

表 20-6　display tcp verbose コマンドの表示情報の説明

フィールド	説明
TCP inpcb number	TCPタイプinternetプロトコル制御ブロック数
tcpcb number	TCP制御ブロック数(TIME_WAIT状態のTCPには、このカウントはありません。)
Connection info	接続情報:ソースIPアドレスとポート番号、宛先IPアドレスとポート番号
Creator	socketを作成したタスクの名前。カッコ内は作成者のプロセス番号
State	socketのステータス。次を含みます。 ● NOFDREF:ユーザが終了しました ● ISCONNECTED:接続が確立されました ● ISCONNECTING:接続を確立中 ● ISDISCONNECTING:切断中 ● ISDISCONNECTED:接続が切断されました ● ISPCBSYNCING:internetプロトコル制御ブロックを同期中 ● ISSMOOTHING:スムージング ● N/A:上記の状態ではありません

フィールド	説明
Options	socketのオプション: • SO_DEBUG:ソケットのデバッグ情報を記録します。 • SO_ACCEPTCONN:serverエンドリスニング接続リクエスト • SO_REUSEADDR:ローカルアドレスの再使用を許可する • SO_KEEPALIVE:プロトコルはアイドル状態の接続を問い合わせる必要があります • SO_DONTROUTE:宛先アドレスが直接ネットワークに接続されているため、ルーティングテーブルを調べないように設定します。 • SO_BROADCAST:ソケットサポートブロードキャストメッセージ • SO_LINGER:ソケットは閉じられているが、まだ残りのデータを送信している • SO_OOBINLINE:帯域外データをインラインで保存 • SO_REUSEPORT:ローカル・ポートの再使用を許可 • SO_TIMESTAMP:接続されていないプロトコルでのみ有効な、ミリ秒単位の着信ロギング・タイムスタンプ • SO_TIMESTAMPNS:タイムスタンプオプションと同様に、ナノ秒までの正確な時間 • SO_KEEPALIVETIME:アイドルプローブ時間の設定 • N/A:オプションが設定されていません
Error	socket接続に影響するエラーコード
Receiving buffer (cc/hiwat/lowat/drop/state)	受信バッファ情報は、現在の使用領域、最大領域、最小領域、ドロップ数、および状態でかっこで囲まれます。状態には次の値があります。 • CANTSENDMORE:データをピアに送信できない • CANTRCVMORE:ピアからデータを受信できない • N/A:上記の状態ではありません
Sending buffer (cc/hiwat/lowat/state)	送信バッファ情報は、現在の使用領域、最大領域、最小領域、ステータスで囲まれます。ステータスには次の値があります。 • CANTSENDMORE:データをピアに送信できない • CANTRCVMORE:ピアからデータを受信できない • N/A:上記の状態ではありません

フィールド	説明
Type	使用されるsocket型は、次のいずれかの値を取ります。 • 1:SOCK_STREAM、ストリームモード、信頼性の高いバイトストリームを提供します。TCPプロトコルはこのタイプを使用します。 • 2:SOCK_DGRAM、データグラムモードの通信。UDPプロトコルはこのタイプを使用します。 • 3:SOCK_RAW、RAWモードの通信方式 • N/A:上記のタイプではありません
Protocol	socketのプロトコル番号を使用
NAT kernel port	NATモジュールのTCPカーネル状態のポートが0の場合は、NAT機能がオンになっていません
Inpcb flags	Internetプロトコル制御ブロック内のタグ。値は次のとおりです。 • INP_RECVOPTS:受信IPオプション • INP_RECVRETOPTS:応答を受信するIPオプション • INP_RECVDSTADDR:宛先IPアドレスの受信 • INP_HDRINCL:IPヘッダ全体をユーザが指定します。 • INP_REUSEADDR:アドレスの再使用 • INP_REUSEPORT:ポート番号の再使用 • INP_ANONPORT:ユーザがポートを指定していません • INP_RECVIF:メッセージ受信時にメッセージを記録するための入力インタフェース • INP_RECVTTL:メッセージを送信するTTL、UDPとRawIPのみサポート • INP_DONTFRAG:シャード不可フラグの設定 • INP_ROUTER_ALERT:ルータ警告オプションを含むメッセージを受信します。RawIPのみサポートされます。 • INP_PROTOCOL_PACKET:メッセージがプロトコル・メッセージであることを示します。 • INP_RCVVLANID:受信メッセージのVLAN ID、UDPとRawIPのみサポート • INP_RCVMACADDR:受信メッセージのMAC • INP_RECVTOS:メッセージを運ぶTOS、UDPとRawIPのみサポート • N/A:上記のタグではありません

フィールド	説明
Inpcb extflag	Internetプロトコル制御ブロック内の拡張タグ。タグの値は次のとおりです。 • INP_EXTRCVPVCIDX:メッセージ受信時にメッセージを記録するPVCインデックス • INP_RCVPWID:メッセージ受信時にメッセージを記録するPW ID • INP_EXTDONTDROP:メッセージの受信時にメッセージを破棄しないように設定する • N/A:上記のタグではありません
Inpcb vflag	Internetプロトコル制御ブロック内のIPバージョンタグは、次の値で構成されます。 • INP_IPv 4:IPv 4との通信に使用 • N/A:上記のタグではありません
TTL	Internetプロトコル制御ブロック中の生存期間、括弧内は最小生存期間
Connection state	次のTCP接続ステータス。 • CLOSED:クライアントから切断接続要求の応答を受信した後のサーバの状態 • LISTEN:接続要求を待機しているサーバの状態 • SYN_SENT:クライアントが接続要求を発行してサーバからの応答を待っている状態 • SYN_RCVD:サーバがクライアント接続リクエストを受信したときの状態 • ESTABLISHED:サーバとクライアントの両方が接続され、双方向のデータ転送が可能な状態 • CLOSE_WAIT:サーバがクライアントから切断要求を受信したときの状態 • FIN_WAIT_1:クライアントが接続クローズ要求を発行してサーバからの応答を待っている状態 • CLOSING:接続のクローズ要求がピアに発行された後、ピアの応答を待っている間に、接続のクローズ要求がピアから受信されたときの状態 • LAST_ACK:サーバがクライアントにクローズ接続要求を出して応答を待っている状態 • FIN_WAIT_2:クライアントがサーバダウン接続応答を受信した後の状態 • TIME_WAIT:クライアントがサーバから切断接続要求を受信した後の状態

フィールド	説明
TCP options	TCPのオプション・タイプは次のとおりです。 • TF_SIGNATURE:イネーブルキー • TF_NODELAY:遅延ACKをオフにする • TF_BINDFOREIGNADDR:ピアIPアドレスのバインド • TF_NSR:有効化TCP NSR • TF_REQ_SCALE:Enable Window Zoom Factorオプション • TF_REQ_TSTMP:タイムスタンプオプションを有効にする • TF_SACK_PERMIT:選択的ACKオプションを有効にする • TF_ENHANCED_AUTH:拡張認証オプションを有効にする • TF_PMTU:有効Path MTUプローブ
NSR state	TCP接続のNSR状態。可能な状態は次のとおりです。 • CLOSED:(初期値)ステータスをオフにする • CLOSING:接続受付クローズ状態 • ENABLED:バックアップ機能の状態を有効にする • OPEN OPEN:接続開始同期ステータス • PENDING:接続判定状態 • READY:接続バックアップ準備状態 • SMOOTH:接続スムージング状態 役割:Mはプライマリ接続、Sはバックアップ接続
Sending VRF	(未サポート)送信インスタンス
Receiving VRF	(未サポート)受入例

20.1.7 display udp

Syntax

display udp

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display udp コマンドを使用して、UDP 接続サマリー情報を表示します。

display udp コマンドは、UDP 接続のサマリー情報を表示します。この情報には、ローカル IP アドレスとポート番号、ピア IP アドレスとポート番号などの情報が含まれます。

例

#UDP 接続サマリー情報を表示します。

<Sysname> display udp

```
 #: Kernel UDP connection
 Local Addr:port          Foreign Addr:port        PCB
 0.0.0.0:69               0.0.0.0:0                0x0000000000000003
#1.0.0.1:179              0.0.0.0:0                N/A
 192.168.20.200:1024      192.168.20.14:69         0x0000000000000002
```

表 20-7　display udp コマンドの表示情報の説明

フィールド	説明
#	接続の前にこのIDがある場合は、UDP接続がComwareカーネルによって使用される接続であることを示します。
Local Addr:port	ローカルIPアドレスとポート番号
Foreign Addr:port	ピアIPアドレスとポート番号
PCB	プロトコル制御ブロックインデックス

20.1.8 display udp statistics

Syntax

display udp statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

UDP トラフィック統計情報を表示するには、**display udp statistics** コマンドを使用します。

display udp statistics コマンドを使用して、送受信されるさまざまな UDP メッセージ情報を含む UDP トラフィック統計情報を表示します。

例

#UDP トラフィックの統計情報を表示します。

<Sysname> display udp statistics

Received packets:

Total: 240

checksum error: 0, no checksum: 0

shorter than header: 0, data length larger than packet: 0

no socket on port(unicast): 0

no socket on port(broadcast/multicast): 240

not delivered, input socket full: 0 ;kenerl buff full: 0

Sent packets:

Total: 0

表 20-8　display udp statistics コマンドの表示情報の説明

フィールド	説明
Received packets:	次のようなメッセージを受信します。 • Total:受信されたUDPメッセージの合計数 • checksum error:チェックサムでエラーが発生したメッセージの数 • no checksum:チェックサムのないメッセージ数 • shorter than header:メッセージ長がヘッダ部より短いメッセージ数 • data length larger than packet:メッセージデータ長がメッセージ長を超えるメッセージ数 • no socket on port (unicast):ポート上のsocketなしユニキャストメッセージ数 • no socket on port (broadcast/multicast):ポート上のsocketなしのブロードキャストおよびマルチキャストメッセージ数 • not delivered, input socket full:xxx;kenerl buff full:yyy:socketバッファがいっぱいになったために上位層に転送されなかったメッセージ数xxxカーネル送信バッファがいっぱいになったために破棄されたメッセージ数yyy
Sent packets:	Totalを含む送信メッセージは、送信されたUDPメッセージの合計数を示します。

関連コマンド

- **reset udp statistics**

20.1.9 display udp verbose

Syntax

display udp verbose [**pcb** *pcb-index*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display udp verbose コマンドは、socket の作成者、状態、オプション、タイプ、使用されているプロトコル番号、UDP 接続の送信元 IP アドレスとポート番号、宛先 IP アドレスとポート番号などの情報を含む UDP 接続の詳細を表示します。

例

#UDP 接続の詳細を表示します。

<Sysname> display udp verbose

Total UDP socket number: 1

Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0

Creator: sock_test_mips[250]

State: N/A

Options: N/A

Error: 0

Receiving buffer(cc/hiwat/lowat/drop/full/state): 0 / 41600 / 1 / 0 / 0 / N/A

Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A

Type: 2

Protocol: 17

Inpcb flags: N/A

Inpcb extflag: N/A

Inpcb vflag: INP_IPV4

TTL: 255(minimum TTL: 0)

Sending VRF: 0

Receiving VRF: 0xffff

表 20-9　display udp verbose コマンドの表示情報の説明

フィールド	説明
Total UDP socket number	UDP socket合計
Connection info	接続情報:ソースIPアドレスとポート番号、宛先IPアドレスとポート番号
Creator	socketを作成したタスクの名前。カッコ内は作成者のプロセス番号

フィールド	説明
State	socketの状態。可能な状態は次のとおりです。 • NOFDREF:ユーザが終了しました • ISCONNECTED:接続が確立されました • ISCONNECTING:接続を確立中 • ISDISCONNECTING:切断中 • ISDISCONNECTED:接続が切断されました • ISPCBSYNCING:internetプロトコル制御ブロックを同期中 • ISSMOOTHING:スムージング • N/A:上記の状態ではありません
Options	socketのオプションは、次のとおりです。 • SO_DEBUG:ソケットのデバッグ情報を記録します。 • SO_ACCEPTCONN:serverエンドリスニング接続リクエスト • SO_REUSEADDR:ローカルアドレスの再使用を許可する • SO_KEEPALIVE:プロトコルはアイドル状態の接続を問い合わせる必要があります • SO_DONTROUTE:宛先アドレスが直接ネットワークに接続されているため、ルーティングテーブルを調べないように設定します。 • SO_BROADCAST:ソケットサポートブロードキャストメッセージ • SO_LINGER:ソケットは閉じられているが、まだ残りのデータを送信している • SO_OOBINLINE:帯域外データをインラインで保存 • SO_REUSEPORT:ローカル・ポートの再使用を許可 • SO_TIMESTAMP:接続されていないプロトコルでのみ有効な、ミリ秒単位の着信ロギング・タイムスタンプ • SO_TIMESTAMPNS:タイムスタンプオプションと同様の機能で、ナノ秒までの正確な時間 • N/A:オプションが設定されていません
Error	socket接続に影響するエラーコード

フィールド	説明
Receiving buffer (cc/hiwat/lowat/drop/full/state)	受信バッファ情報は、現在の使用領域、最大領域、最小領域、パケット損失数、カーネル送信バッファがいっぱいになったパケット損失数、状態であり、状態は以下の値をとる. ● CANTSENDMORE:データをピアに送信できない ● CANTRCVMORE:ピアからデータを受信できない ● N/A:上記の状態ではありません
Sending buffer (cc/hiwat/lowat/state)	送信バッファ情報は、現在の使用領域、最大領域、最小領域、およびステータスでかっこで囲まれます。ステータスには次の値があります。 ● CANTSENDMORE:データをピアに送信できない ● CANTRCVMORE:ピアからデータを受信できない ● N/A:上記の状態ではありません
Type	使用されるsocket型は、次の値を取ります。 ● 1:SOCK_STREAM、ストリームモード、信頼性の高いバイトストリームを提供します。TCPプロトコルはこのタイプを使用します。 ● 2:SOCK_DGRAM、データグラムモードの通信。UDPプロトコルはこのタイプを使用します。 ● 3:SOCK_RAW、RAWモードの通信方式 ● N/A:上記のタイプではありません
Protocol	socketのプロトコル番号を使用

フィールド	説明
Inpcb flags	Internetプロトコル制御ブロック内のタグ。値は次のとおりです。 • INP_RECVOPTS:受信IPオプション • INP_RECVRETOPTS:応答を受信するIPオプション • INP_RECVDSTADDR:宛先IPアドレスの受信 • INP_HDRINCL:IPヘッダ全体をユーザが指定します。 • INP_REUSEADDR:アドレスの再使用 • INP_REUSEPORT:ポート番号の再使用 • INP_ANONPORT:ユーザがポートを指定していません • INP_RECVIF:メッセージ受信時にメッセージを記録するための入力インタフェース • INP_RECVTTL:メッセージを送信するTTL、UDPとRawIPのみサポート • INP_DONTFRAG:シャード不可フラグの設定 • INP_ROUTER_ALERT:ルータ警告オプションを含むメッセージを受信します。RawIPのみサポートされます。 • INP_PROTOCOL_PACKET:メッセージがプロトコル・メッセージであることを示します。 • INP_RCVVLANID:受信メッセージのVLAN ID、UDPとRawIPのみサポート • INP_RCVMACADDR:受信メッセージのMAC • INP_RECVTOS:メッセージを運ぶTOS、UDPとRawIPのみサポート • N/A:上記のタグではありません
Inpcb extflag	Internetプロトコル制御ブロック内の拡張タグ。タグの値は次のとおりです。 • INP_EXTRCVPVCIDX:メッセージ受信時にメッセージを記録するPVCインデックス • INP_RCVPWID:メッセージ受信時にメッセージを記録するPW ID • N/A:上記のタグではありません
Inpcb vflag	Internetプロトコル制御ブロック内のIPバージョンタグ。タグの値は次のとおりです。 • INP_IPv 4:IPv 4との通信に使用 • N/A:上記のタグではありません
TTL	Internetプロトコル制御ブロック中の生存期間、括弧内は最小生存期間
Sending VRF	(未サポート)送信インスタンス

フィールド	説明
Receiving VRF	(未サポート)受入例

20.1.10 ip forward-broadcast

Syntax

ip forward-broadcast

undo ip forward-broadcast

デフォルト

デバイスは、直接接続されたセグメントのダイレクトブロードキャストメッセージの転送を禁止します。

View

Interface view

定義済みユーザロール

network-admin

説明

ip forward-broadcast コマンドを使用して、インタフェースが直接接続されたセグメントを転送できるように、ダイレクトブロードキャストメッセージを設定します。

undo ip forward-broadcast コマンドを使用して、インタフェースが直接接続されたセグメントのダイレクトブロードキャストメッセージを転送できないようにします。

ディレクテッドブロードキャストメッセージは、特定のネットワークに送信されるブロードキャストメッセージです。このメッセージの宛先 IP アドレスのネットワーク番号フィールドは特定のネットワークのネットワーク番号であり、ホスト番号フィールドはすべて 1 である。

このコマンドがインタフェースで設定されている場合、ダイレクトブロードキャストメッセージを転送すると、デバイスは、このインタフェースの直接接続セグメントの宛先アドレスを持つダイレクトブロードキャストメッセージを他のインタフェースから受信すると、そのようなメッセージをこのインタフェースから転送します。

例

#VLAN インタフェース 2 が直接接続セグメントを対象とした指向性ブロードキャストメッセージを転送できるように設定します。

<Sysname> system-view

[Sysname] interface vlan-interface 2

[Sysname-Vlan-interface2] ip forward-broadcast

20.1.11 ip icmp error-interval

Syntax

ip icmp error-interval *interval* [*bucketsize*]

undo ip icmp error-interval

デフォルト

トークン更新サイクルは 100 ミリ秒で、トークンバケット容量は 10 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:0~2147483647 の範囲の値をミリ秒単位で取得するトークンリフレッシュサイクル。0 時の値をとり、 ICMP エラーメッセージの送信を制限しないことを示す。

bucketsize: トークンバケットに格納されているトークンの数。範囲は 1~200 です。

説明

ip icmp error-interval は、ICMP エラーメッセージの送信に対応するトークンリフレッシュサイクルとトークンバケットサイズを設定するために使用されます。

undo ip icmp error-interval は、デフォルトの状態に戻す。

ネットワーク内で短時間に送信される ICMP エラーメッセージが多すぎると、ネットワークが輻輳する可能性があります。これを回避するために、ユーザは、現在トークンバケットアルゴリズムを使用して実装されている、指定された時間内にデバイスが送信する ICMP エラーメッセージの最大数を制御することができる。

ユーザはトークンバケットの容量、つまりトークンバケットに同時に格納できるトークンの数を設定できます。また、トークンバケットの更新サイクル、つまり、トークンバケット内のトークン数が設定された容量に達するまで、トークンがトークンバケットに発行される間隔も設定できます。トークンは、1 つの ICMP エラーメッセージが送信されるたびにトークンバケットから 1 つのトークンが削除される ICMP エラーメッセージの送信を許可することを意味します。連続して送信される ICMP エラーメッセージがトークンバケットの容量を超える場合、設定されたリフレッシュレートで新しいトークンがトークンバケットに配置されるまで、後続の ICMP エラーメッセージは送信されません。

例

#ICMP エラーメッセージを送信するようにデバイスを設定するトークンリフレッシュサイクルは 200 ミリ秒で、トークンバケット容量は 40 です。

<Sysname> system-view

[Sysname] ip icmp error-interval 200 40

20.1.12 ip mtu

Syntax

ip mtu *mtu-size*

undo ip mtu

デフォルト

IPv 4 メッセージを送信するインタフェースの MTU が設定されていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

mtu-size:MTU のサイズはバイト単位で、このパラメータの範囲はインタフェースのタイプに依存します。デバイスの実際の状態に基づいてください。

説明

ip mtu コマンドは、IPv 4 メッセージを送信するインタフェースの MTU を設定します。

undo ip mtu コマンドを使用して、デフォルトの状態を復元します。

デバイスがメッセージを受信したときに、転送インタフェースの送信 IPv 4 メッセージの MTU 値よりも大きいメッセージ長が検出された場合は、次の処理が行われます。

- メッセージがフラグメント化を許可しない場合、メッセージは破棄されます。
- メッセージがフラグメント化を許可する場合、メッセージはフラグメント化されて転送されます。

転送デバイスが転送中にパケットをフラグメント化および再構成する必要性を軽減し、ネットワークリソースをより効率的に使用するには、フラグメントの発生を減らすために、実際のネットワーク環境に合わせて適切なインタフェースを設定し、IPv 4 メッセージの MTU 値を送信します。

現在のインタフェースが **mtu** コマンドと **ip mtu** コマンドの両方をサポートしている場合、デバイスは、**ip mtu** コマンドで設定されたインタフェースに IPv 4 メッセージの MTU 値を送信してメッセージをフラグメント化し、**mtu** コマンドで設定された MTU 値に基づいてメッセージをフラグメント化しません。

例

#VLAN インタフェース 100 で送信される IPv 4 メッセージの MTU 値を 1280 バイトに設定します。

<Sysname> system-view

[Sysname] interface vlan-interface 100

[Sysname-Vlan-interface100] ip mtu 1280

20.1.13 ip redirects enable

Syntax

ip redirects enable

undo ip redirects enable

デフォルト

ICMP リダイレクトメッセージ送信機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

ip redirects enable コマンドを使用して、デバイスの ICMP リダイレクトメッセージの送信機能を有効にします。

undo ip redirects enable コマンドを使用して、デバイスの ICMP リダイレクトメッセージの送信機能をオフにします。

ICMP リダイレクトメッセージ送信機能は、ホストの管理を簡素化し、ルーティング情報が少ないホストは、最適なルートを見つけるために、より完全なルーティングテーブルを確立します。

ホストが起動すると、そのルーティングテーブルには、デフォルトゲートウェイへのデフォルトルートが 1 つしかない場合があります。一定の条件が満たされると、デフォルトゲートウェイは ICMP リダイレクトメッセージを送信元ホストに送信し、次のメッセージ送信のために正しいネクストホップを再選択するようにホストに通知する。

次の条件の両方が満たされると、デバイスは ICMP リダイレクトメッセージを送信します。

- データグラムを受信および転送するインタフェースは同じインタフェースです。
- メッセージの送信元 IP アドレスと、同じネットワークセグメント上のメッセージ受信インタフェースの IP アドレス;
- データグラムにソースルーティングオプションがありません。

例

#デバイスの ICMP リダイレクトメッセージ送信機能をオンにします。

<Sysname> system-view

[Sysname] ip redirects enable

20.1.14 ip ttl-expires enable

Syntax

ip ttl-expires enable

undo ip ttl-expires enable

デフォルト

ICMP タイムアウトメッセージ送信機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

ip ttl-expires enable コマンドは、デバイスの ICMP タイムアウトメッセージの送信機能を有効にします。

undo ip ttl-expires enable コマンドは、デバイスの ICMP タイムアウトメッセージの送信機能を無効にするために使用します。

ICMP タイムアウトメッセージ送信機能は、デバイスが IP データメッセージを受信した後、タイムアウトエラーが発生すると、メッセージを破棄して送信元に ICMP タイムアウトエラーを送信する。

デバイスは、次の条件が満たされると ICMP タイムアウトメッセージを送信します。

- デバイスが IP データグラムを受信した後、メッセージの宛先がローカルではなく、メッセージの TTL フィールドが 1 の場合、ICMP エラーメッセージが送信「TTL タイムアウト」されます。
- デバイスは、宛先アドレスがローカルである IP データグラムの最初のフラグメントを受信すると、タイマを開始し、すべてのフラグメントが到着する前にタイマが切れると、ICMP エラーメッセージを送信「再編成タイムアウト」します。

ICMP タイムアウトメッセージの送信機能をオフにすると、デバイスは ICMP エラーメッセージを送信「TTL タイムアウト」しなくなりますが、「再編成タイムアウト」 ICMP エラーメッセージは正常に送信されます。

例

#デバイスの ICMP タイムアウトメッセージ送信機能をオンにします。

<Sysname> system-view

[Sysname] ip ttl-expires enable

20.1.15 ip unreachables enable

Syntax

ip unreachables enable

undo ip unreachables enable

デフォルト

ICMP 到達不能メッセージ送信機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

ip unreachables enable コマンドを使用して、デバイスの ICMP 到達不能メッセージの送信機能をオンにします。

undo ip unreachables enable コマンドを使用して、デバイスの ICMP 宛先到達不能メッセージの送信機能をオフにします。

ICMP 到達不能メッセージ送信機能では、デバイスが IP データグラムを受信した後、到達不能エラーが発生すると、ICMP 到達不能エラーメッセージを送信元にドロップして送信します。

デバイスは、次の条件が満たされた場合に宛先到達不能メッセージを送信します。

- デバイスがメッセージを転送するときに、ルーティングテーブルに対応する転送ルートが見つからず、ルーティングテーブルにデフォルトルートがない場合、ICMP エラーメッセージが送信元に送信「ネットワークに到達できません」されます。
- 宛先アドレスがローカルのデータメッセージをデバイスが受信した場合、デバイスがデータメッセージに使用されているトランスポート・レイヤ・プロトコルをサポートしていない場合、ICMP エラーメッセージが送信元に送信「合意に達しない」される;
- デバイスは、宛先アドレスがローカルで、トランスポート層プロトコルが UDP のデータグラムを受信したときに、使用中のプロセスと一致しないポート番号を持つ ICMP エラーメッセージ「ポートは到達不能」を送信元に送信します。
- 送信元が「厳密なソースルーティング」を使用してテキストを送信する場合、中間デバイスは、ソースルートによって指定された次のデバイスが直接接続されているネットワーク上にないことを検出すると、「ソースルーティングに失敗しました」の ICMP エラーメッセージを送信元に送信します。
- デバイスがメッセージを転送するとき、転送インタフェースの MTU がメッセージの長さより小さいが、メッセージがフラグメント化不可に設定されている場合、ICMP

エラーメッセージが送信元に送信「シャーディングが必要ですが、アンシャードビットが設定されています」されます。

例

#デバイスの ICMP 目的到達不能メッセージ送信機能をオンにします。

<Sysname> system-view

[Sysname] ip unreachables enable

20.1.16 reset ip statistics

Syntax

reset ip statistics

View

User view

定義済みユーザロール

network-admin

説明

reset ip statistics コマンドは、IP メッセージの統計情報をクリアするために使用します。

場合によっては、一定時間内にインタフェースの IP パケットの統計情報を集計する必要があるが、その場合は、集計を開始する前に既存の統計情報を消去し、再集計する必要がある。

例

#IP メッセージの統計情報をクリアします。

<Sysname> reset ip statistics

関連コマンド

- **display ip interface (3 層テクノロジー-IP ビジネスコマンドリファレンス/IP アドレス)**
- **display ip statistics**

20.1.17 reset udp statistics

Syntax

reset udp statistics

View

User view

定義済みユーザロール

network-admin

説明

UDP トラフィック統計情報をクリアするには、**reset udp statistics** コマンドを使用します。

例

#UDP トラフィック統計情報をクリアします。

<Sysname> reset udp statistics

関連コマンド

- **display udp statistics**

20.1.18 tcp path-mtu-discovery

Syntax

tcp path-mtu-discovery [**aging** *age-time* | **no-aging**]

undo tcp path-mtu-discovery

デフォルト

TCP 接続の Path MTU プローブ機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

aging *age-time*:Path MTU のエージング時間は、age-time では分単位で 10~30 の値をとり、デフォルトは 10 です。

no-aging:Path MTU エージングなし。

説明

tcp path-mtu-discovery コマンドは、TCP 接続の Path MTU プローブ機能を有効にします。

undo tcp path-mtu-discovery コマンド TCP 接続を閉じるために使用される Path MTU プローブ機能。

TCP 接続の Path MTU 探知機能をオンにした後、新しい TCP 接続はすべて Path MTU 探知属性を携帯し、探知メカニズムによって Path MTU を確定することができ、データ経

路上の最小 MTU によって TCP セグメント長を組織し、最大限にネットワーク資源を利用し、IP シャードの発生を避ける。

TCP 接続の Path MTU プローブを閉じると、システムは実行中のすべての Path MTU タイマを停止します。その後、作成された TCP 接続には Path MTU プローブはありませんが、すでに確立されている TCP 接続の Path MTU プローブは閉じません。

例

#TCP 接続の Path MTU プローブ機能をオンにすると、Path MTU のエージングタイムは 20 分になります。

<Sysname> system-view

[Sysname] tcp path-mtu-discovery aging 20

20.1.19 tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

デフォルト

TCP finwait タイマのタイムアウト時間は 675 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value:TCP finwait タイマのタイムアウト時間は、 763600 の範囲で、単位は秒である。

説明

tcp timer fin-timeout コマンド TCP の finwait タイマータイムアウト時間を設定します。

undo tcp timer fin-timeout コマンドを使用して、デフォルトの状態を復元します。

TCP の接続状態が FIN_WAIT_2 の場合、 finwait タイマを起動し、タイマがタイムアウトするまでにメッセージを受信しなければ TCP 接続を終了する.;FIN メッセージを受信すると、TCP 接続のステータスが TIME_WAIT に変わります。非 FIN メッセージを受信した場合は、最後に受信した非 FIN メッセージから再タイミングを取り、タイムアウト後に接続を中止します。

例

#TCP finwait タイマのタイムアウトを 800 秒に設定します。

<Sysname> system-view

[Sysname] tcp timer fin-timeout 800

20.1.20 tcp timer syn-timeout

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

デフォルト

TCP synwait タイマのタイムアウト時間は 75 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value:TCP synwait タイマのタイムアウト時間は、2600 の範囲で、単位は秒である。

説明

tcp timer syn-timeout コマンド TCP の synwait タイマータイムアウト時間を設定します。

undo tcp timer syn-timeout コマンドを使用して、デフォルトの状態を復元します。

SYN メッセージを送信する場合、TCP は synwait タイマと再送信 SYN メッセージタイマーを起動し、synwait タイマがタイムアウトし、かつ SYN メッセージの再送信が最大回数に達していない場合、デバイスが応答メッセージを受信しなければ、TCP 接続確立は成功しない。synwait タイマがタイムアウトせず、SYN メッセージが最大回数まで再送信された場合、デバイスが応答メッセージを受信しないと、TCP 接続の確立は失敗します。

例

#TCP synwait タイマのタイムアウトを 80 秒に設定します。

<Sysname> system-view

[Sysname] tcp timer syn-timeout 80

20.1.21 tcp window

Syntax

tcp window *window-size*

undo tcp window

デフォルト

TCP 接続の送受信バッファサイズは 63 KB です。

View

System view

定義済みユーザロール

network-admin

パラメータ

window-size:TCP コネクションの送受信バッファサイズを KB (キロバイト)で 5~64 の範囲で指定します。

説明

tcp window コマンドは、TCP 接続の送受信バッファサイズを設定します。

undo tcp window コマンドを使用して、デフォルトの状態を復元します。

例

#TCP 接続の送受信バッファサイズを 6 KB に設定します。

<Sysname> system-view

[Sysname] tcp window 6

目次

このセクションのページは **5-x-x** です。

21 章 NAT 21-1
21.1 NAT 設定コマンド 21-1
21.1.1 address 21-1
21.1.2 block-size 21-2
21.1.3 display nat address-group 21-3
21.1.4 display nat all 21-5
21.1.5 display nat dns-map 21-14
21.1.6 display nat eim 21-15
21.1.7 display nat inbound 21-17
21.1.8 display nat log 21-19
21.1.9 display nat no-pat 21-21
21.1.10 display nat outbound 21-23
21.1.11 display nat outbound port-block-group 21-25
21.1.12 display nat port-block 21-26
21.1.13 display nat port-block-group 21-30
21.1.14 display nat server 21-32
21.1.15 display nat server-group 21-36
21.1.16 display nat session 21-37
21.1.17 display nat static 21-39
21.1.18 display nat statistics 21-42
21.1.19 global-ip-pool 21-44
21.1.20 inside ip 21-46
21.1.21 local-ip-address 21-47
21.1.22 nat address-group 21-48
21.1.23 nat alg 21-49
21.1.24 nat dns-map 21-51
21.1.25 nat inbound 21-52
21.1.26 nat inbound rule move 21-55
21.1.27 nat log enable 21-56
21.1.28 nat log flow-active 21-57
21.1.29 nat log flow-begin 21-58
21.1.30 nat log flow-end 21-59
21.1.31 nat log port-block usage threshold 21-60
21.1.32 nat mapping-behavior endpoint-independent 21-61
21.1.33 nat outbound 21-63
21.1.34 nat outbound port-block-group 21-66

21.1.35 nat outbound rule move 21-67
21.1.36 nat port-block-group 21-68
21.1.37 nat server rule move 21-70
21.1.38 nat server (interface-based NAT) 21-71
21.1.39 nat server-group 21-76
21.1.40 nat static enable 21-77
21.1.41 nat static inbound 21-78
21.1.42 nat static inbound net-to-net 21-80
21.1.43 nat static inbound rule move 21-83
21.1.44 nat static outbound 21-84
21.1.45 nat static outbound net-to-net 21-86
21.1.46 nat static outbound rule move 21-89
21.1.47 nat timestamp delete 21-90
21.1.48 port-block 21-91
21.1.49 port-range 21-92
21.1.50 reset nat session 21-93

21章 NAT

21.1 NAT設定コマンド

21.1.1 address

Syntax

address *start-address end-address*

undo address *start-address end-address*

デフォルト

アドレスメンバが存在しません。

View

NAT address group view

定義済みユーザロール

network-admin

パラメータ

start-address end-address:アドレスメンバの開始 IP アドレスと終了 IP アドレス。end-address は start-address 以上である必要があります。start-address と end-address が同じ場合、アドレスは 1 つだけです。start-address と end-address の間の IP アドレスの数は 256 を超えることはできません。

説明

アドレスメンバを追加するには、**address** コマンドを使用します。

undo address コマンドは、アドレスメンバを削除するために使用します。

1 つの NAT アドレスグループは、複数のアドレスメンバの集合です。外部ネットワークに到着したデータメッセージのアドレス変換が必要な場合、メッセージの送信元アドレスはアドレスメンバ中のいずれかのアドレスに変換される。

同じ NAT アドレスグループ内でこのコマンドを複数回実行して追加したアドレスメンバは、重複してはなりません。

パブリックアドレスのメンバが NAT ポートブロックのスタティックマップのパブリックアドレスのメンバと重複している場合は、NAT ポートブロックのスタティックマップのポート範囲と NAT ポートブロックのダイナミックマップのポート範囲が重複していないことを確認します。そうしないと、ユーザがオンラインになったときに、デバイスが同じパブリック IP アドレスとポートブロックを 2 人の異なるユーザに割り当てた場合、どちらかのユーザの NAT セッションが作成されないことがあります。

例

#NAT アドレスグループ 2 にアドレスメンバを追加します。

<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] address 10.1.1.1 10.1.1.15
[Sysname-address-group-2] address 10.1.1.20 10.1.1.30

関連コマンド

- **nat address-group**

21.1.2 block-size

Syntax

block-size *block-size*

undo block-size

デフォルト

1 つのポートブロックには 256 個のポートが含まれます。

View

NAT port block group view

定義済みユーザロール

network-admin

パラメータ

block-size:ポートブロックサイズは、 1 つのポートブロックに含まれるポート数であり、1max_number の範囲で値をとる。ここで、max_number は 65535 です。

説明

block-size コマンドを使用して、ポートブロックサイズを設定します。

undo block-size コマンドを使用して、デフォルトの状態を復元します。

1 つのポートブロックグループでは、プライベート IP アドレスの数、パブリック IP アドレスの数、およびポート範囲に基づいて、適切なポートブロックサイズ値を決定する必要があります。ポートブロックサイズの値は、パブリックネットワークアドレスのポート範囲の値を超えることはできません。

例

#ポートブロックグループ 1 のポートブロックサイズを 1024 に設定します。

<Sysname> system-view
[Sysname] nat port-block-group 1

[Sysname-port-block-group-1] block-size 1024

関連コマンド

- **nat port-block-group**

21.1.3 display nat address-group

Syntax

display nat address-group [*group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id:アドレスグループの番号。範囲は 0~65535 です。この値を設定しない場合は、すべてのアドレスグループが表示されます。

説明

display nat address-group コマンドを使用して、NAT アドレスグループの設定情報を表示します。

例

#すべてのアドレスグループの設定情報を表示します。

<Sysname> display nat address-group

```
NAT address group information:
  Totally 5 NAT address groups.
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address          End address
      202.110.10.10          202.110.10.15

  Address group 2:
    Port range: 1-65535
    Address information:
      Start address          End address
      202.110.10.20          202.110.10.25
      202.110.10.30          202.110.10.35
```

```
Address group 3:
  Port range: 1024-65535
  Address information:
    Start address          End address
    202.110.10.40          202.110.10.50

Address group 4:
  Port range: 10001-65535
  Port block size: 500
  Extended block number: 1
  Address information:
    Start address          End address
    202.110.10.60          202.110.10.65

Address group 6:
  Port range: 1-65535
  Address information:
    Start address          End address
    ---                    ---
```

#指定したアドレスグループの構成情報を表示します。

```
<Sysname> display nat address-group 1
Address group 1:
  Port range: 1-65535
  Address information:
    Start address          End address
    202.110.10.10          202.110.10.15
```

表 21-1 display nat address-group コマンドの表示情報の説明

フィールド	説明
NAT address group information	NATアドレスグループ情報
Totally n NAT address groups	現在n個のアドレスグループがあります
Address group	アドレスグループの番号
Port range	アドレスのポート範囲
Block size	ポートブロックサイズ。構成されていない場合は表示されません。
Extended block number	インクリメンタルポートブロック数。構成されていない場合は表示されません。
Address information	アドレスグループメンバ情報
Start address	アドレスグループメンバの開始アドレス。構成されていない場合は、 「---」 と表示されます。

フィールド	説明
End address	アドレスグループメンバの終了アドレス。構成されていない場合は、 「---」 と表示されます。

関連コマンド

- **nat address-group**

21.1.4 display nat all

Syntax

display nat all

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat all コマンドを使用して、すべての NAT 設定情報を表示します。

例

#すべての NAT 設定情報を表示します。

<Sysname> display nat all

```
NAT address group information:
  Totally 5 NAT address groups.
  Address group 1:
    Port range: 1-65535
    Address information:
      Start address          End address
      202.110.10.10          202.110.10.15

  Address group 2:
    Port range: 1-65535
    Address information:
      Start address          End address
      202.110.10.20          202.110.10.25
      202.110.10.30          202.110.10.35

  Address group 3:
```

```
    Port range: 1024-65535
    Address information:
      Start address          End address
      202.110.10.40          202.110.10.50

  Address group 4:
    Port range: 10001-65535
    Port block size: 500
    Extended block number: 1
    Address information:
      Start address          End address
      202.110.10.60          202.110.10.65

  Address group 6:
    Port range: 1-65535
    Address information:
      Start address          End address
      ---                    ---

NAT server group information:
  Totally 3 NAT server groups.
  Group Number      Inside IP          Port       Weight
  1                 192.168.0.26       23         100
                    192.168.0.27       23         500
  2                 ---                ---        ---
  3                 192.168.0.26       69         100

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2038          Address group: 2       Add route: Y
    NO-PAT:Y           Reversible: N
    VPN instance: vpn_nat
    Rule name: abc
    Priority: 1000
    Config status: Active

NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: GigabitEthernet1/0/1
    ACL: 2036          Address group: 1       Port-preserved: Y
    NO-PAT: N          Reversible: N
    Rule name: def
```

```
    Priority: 22
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: address group, and ACL.

  Interface: GigabitEthernet1/0/1
    ACL: 2037            Address group: 1        Port-preserved: N
    NO-PAT: Y            Reversible: Y
    VPN instance: vpn_nat
    Rule name: rabbit
    Priority: 100
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

NAT internal server information:
  Totally 5 internal servers.
  Interface: GigabitEthernet1/0/3
    Global ACL      : 2000
    Local IP/port : 192.168.10.1/23
    Config status : Active
    Rule name       : rule1
    Priority        : 1000

  Interface: GigabitEthernet1/0/3
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    ACL             : 2000
    Rule name       : rule2
    Config status : Active

  Interface: GigabitEthernet1/0/4
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23-30
    Local IP/port : 192.168.10.15-192.168.10.22/23
    Global VPN      : vpn1
    Local VPN       : vpn3
    Rule name       : rule3
    Config status : Active

  Interface: GigabitEthernet1/0/4
    Protocol: 255(Reserved)
```

Global IP/port: 50.1.1.100/---
Local IP/port : 192.168.10.150/---
Global VPN : vpn2
Local VPN : vpn4
ACL : 3000
Rule name : rule4
Config status : Inactive
Reasons for inactive status:
The following items don't exist or aren't effective: local VPN, and ACL.

Interface: GigabitEthernet1/0/5
Protocol: 17(UDP)
Global IP/port: 50.1.1.2/23
Local IP/port : server group 1
1.1.1.1/21 (Connections: 10)
192.168.100.200/80 (Connections: 20)
Global VPN : vpn1
Local VPN : vpn3
Rule name : rule5
Config status : Active

NAT Instance: instance1
Protocol: 6(TCP)
Global IP/port: 1.1.1.1/0
Local IP/port : 2.2.2.2/0
Config status : Active

Static NAT mappings:
Totally 2 inbound static NAT mappings.
Net-to-net:
Global IP : 2.2.2.1 – 2.2.2.255
Local IP : 1.1.1.0
Netmask : 255.255.255.0
Global VPN : vpn2
Local VPN : vpn1
ACL : 3000
Reversible : Y
Rule name : rulestatic
Priority : 4
Config status: Active

IP-to-IP:
Global IP : 5.5.5.5

Local IP : 4.4.4.4
Global VPN : vpn3
Local VPN : vpn4
ACL : 2001
Reversible : Y
Rule name : ruleiptoip
Priority : 4
Config status: Inactive
Reasons for inactive status:
The following items don't exist or aren't effective: local VPN, global VPN, and ACL.

Totally 2 outbound static NAT mappings.
Net-to-net:
Local IP : 1.1.1.1 - 1.1.1.255
Global IP : 2.2.2.0
Netmask : 255.255.255.0
Local VPN : vpn1
Global VPN : vpn2
ACL : 3000
Reversible : Y
Rule name : rulenettonet
Priority : 5
Config status: Active

IP-to-IP:
Local IP : 4.4.4.4
Global IP : 5.5.5.5
Local VPN : vpn1
Global VPN : vpn2
ACL: : 2001
Reversible : Y
Rule name : rule10
Priority : 6
Config status: Inactive
Reasons for inactive status:
The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
Totally 2 interfaces enabled with static NAT.
Interface: GigabitEthernet1/0/2
Config status: Active

Interface: GigabitEthernet1/0/3

```
    Config status: Active

NAT DNS mappings:
  Totally 2 NAT DNS mappings.
  Domain name   : www.server.com
  Global IP     : 6.6.6.6
  Global port   : 23
  Protocol      : TCP(6)
  Config status: Active

  Domain name   : www.service.com
  Global IP     : ---
  Global port   : 12
  Protocol      : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.

NAT logging:
  Log enable                : Enabled
  Flow-begin                : Disabled
  Flow-end                  : Disabled
  Flow-active               : Disabled
  Port-block-assign         : Disabled
  Port-block-withdraw       : Disabled
  Port-alloc-fail           : Enabled
  Port-block-alloc-fail     : Disabled
  Port-usage                : Disabled
  Port-block-usage          : Enabled(40%)

NAT hairpinning:
  Totally 2 interfaces enabled with NAT hairpinning.
  Interface: GigabitEthernet1/0/1
    Config status: Active

  Interface: GigabitEthernet1/0/2
    Config status: Active

NAT mapping behavior:
  Mapping mode : Endpoint-Independent
  ACL          : 2050
  Config status: Active
```

```
NAT ALG:
  DNS          : Enabled
  FTP          : Enabled
  H323         : Disabled
  ICMP-ERROR : Enabled
  ILS          : Disabled
  MGCP         : Disabled
  NBT          : Disabled
  PPTP         : Enabled
  RTSP         : Enabled
  RSH          : Disabled
  SCCP         : Disabled
  SIP          : Disabled
  SQLNET       : Disabled
  TFTP         : Disabled
  XDMCP        : Disabled

NAT port block group information:
  Totally 3 NAT port block groups.
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address          VPN instance
      172.16.1.1           172.16.1.254         ---
      192.168.1.1          192.168.1.254        vpna
      192.168.3.1          192.168.3.254        vpna
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25

  Port block group 2:
    Port range: 10001-30000
    Block size: 500
    Local IP address information:
      Start address        End address          VPN instance
      10.1.1.1             10.1.10.255          vpnb
    Global IP pool information:
      Start address        End address
      202.10.10.101        202.10.10.120

  Port block group 3:
```

```
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address          End address            VPN instance
      ---                    ---                    ---
    Global IP pool information:
      Start address          End address
      ---                    ---

NAT outbound port block group information:
  Totally 2 outbound port block group items.
  Interface: GigabitEthernet1/0/2
    port-block-group: 2
    Rule name          : ruleoutbound1
    Priority           : 4
    Config status      : Active

  Interface: GigabitEthernet1/0/2
    port-block-group: 10
    Rule name          : ruleoutbound2
    Priority           : 6
    Config status      : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: port block group.
```

上記の表示情報は、現在のすべての NAT 設定情報のコレクションです。一部の NAT 設定(nat address-group、nat server-group、nat inbound、nat outbound、nat server、nat static、nat static net-to-net、nat static enable、nat dns-map、nat log、nat port-block-group、nat outbound port-block-group)には独自の表示コマンドがあり、ここに表示される情報の形式は各コマンドに対応する表示情報の形式と同じであるため、これらの設定の表示フィールドの意味についてはここでは詳しく説明しません。必要に応じて、個別の表示コマンドを参照してください。次の表では、関連する表示コマンドについて説明し、nat hairpin enable と nat mapping-behavior についてのみ説明します。

表 21-2 display nat all コマンドの表示情報の説明

フィールド	説明
NAT address group information	NATアドレスグループの設定情報、フィールドの詳細については、「表 21-1」を参照してください。
NAT server group information	NAT内部サーバグループの設定情報、フィールドの詳細については、「表 21-14」を参照してください。
NAT inbound information:	着信方向ダイナミックアドレス変換の設定情報、フィールドの詳細については、「表 21-5」を参照してください。

フィールド	説明
NAT outbound information	送信方向ダイナミックアドレス変換の設定情報、フィールドの詳細については、「表 21-8」を参照してください。
NAT internal server information	NAT内部サーバの設定情報、フィールドの詳細については、「表 21-13」を参照してください。
Static NAT mappings	静的アドレス変換の構成情報、フィールドの詳細については、「表 21-16」を参照してください。
NAT DNS mappings	NAT DNS mappingの構成情報、詳細なフィールド説明「表 21-3」を参照してください。
NAT logging	NATログ機能の設定については、「表 21-6」を参照してください。
NAT hairpinning	NAT hairpinの機能
Totally n interfaces enabled NAT hairpinning	現在n個のインタフェースが起動していますNAT hairpin
Interface	NAT hairpin機能を有効にするインタフェース
Rule name	NATルールの名前
Priority	NATルールの一致の優先順位
Config status	NAT hairpin構成のステータスの表示
NAT mapping behavior	PAT方式におけるアドレス変換モード • Endpoint-Independent:ピアアドレスとポートを問わない変換モードを示します。 • Address and Port-Dependent:ピアアドレスとポートの変換モードを示します。
ACL	参照先のACL番号または名前。構成されていない場合は、「---」と表示されます。
Config status	NAT mapping behavior構成のステータスの表示 • Active:有効 • Inactive:無効
Reasons for inactive status	Config statusフィールドがInactiveの場合は、NAT mapping behavior設定が有効でない理由が表示されます。 • The following items don't exist or aren't effective:ACL:参照 ACL が存在しません
NAT ALG	各プロトコルのNAT ALG機能のオン/オフ情報
NAT port block group information	NATポートブロックグループの設定情報、フィールドの詳細については、「表 21-12」を参照してください。
NAT outbound port block group information	NATポートブロックスタティックマッピングの設定情報、フィールドの詳細については、「表 21-9」を参照してください。

21.1.5 display nat dns-map

Syntax

display nat dns-map

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat dns-map コマンドは、NAT DNS mapping 構成情報を表示するために使用します。

例

#NAT DNS mapping の設定情報を表示します。

<Sysname> display nat dns-map
NAT DNS mapping information:
  Totally 2 NAT DNS mappings.
  Domain name : www.server.com
  Global IP   : 6.6.6.6
  Global port : 23
  Protocol   : TCP(6)
  Config status: Active

  Domain name : www.service.com
  Global IP   : ---
  Global port : 12
  Protocol   : TCP(6)
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: interface IP address.

表 21-3 display nat dns-map コマンドの表示情報の説明

フィールド	説明
NAT DNS mapping information	NAT DNS mapping設定情報
Totally n NAT DNS mappings	現在n個のDNS mapping構成
Domain name	DNSドメイン名

フィールド	説明
Global IP	外部ネットワークアドレス。設定でEasy IPモードを使用している場合は、ここに指定されたインタフェースのアドレスが表示されます。「---」は、インタフェースに外部ネットワークアドレスが設定されていないことを示します。
Global port	外部ネットワークポート番号
Protocol	基本契約名および基本契約番号
Config status	DNS mapping構成のステータスの表示 • Active:有効 • Inactive:無効
Reasons for inactive status	Config statusフィールドがInactiveの場合は、DNS mapping設定が有効でない理由が表示されます。 • The following items don't exist or aren't effective:interface IP address:参照インタフェースの IP アドレスが設定されていません

関連コマンド

- **nat dns-map**

21.1.6 display nat eim

Syntax

display nat eim [**protocol** { **tcp** | **udp** }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

protocol:指定したプロトコルタイプの EIM テーブルエントリ情報を表示します。

tcp:TCP プロトコルタイプの EIM テーブルエントリ情報を表示します。

udp:UDP プロトコルタイプの EIM テーブルエントリ情報を表示します。

説明

display nat eim コマンドは、NAT EIM テーブルエントリ情報を表示します。

EIM トリプレットは、メッセージが Endpoint-Independent Mapping 方式の PAT 変換を行う際に生成され、イントラネットとエクストラネットの変換関係(イントラネットアドレ

スとポート<--> NAT アドレスとポート)を記述するものであり、このエントリには以下の 2 つの役割がある.

- 同じ送信元アドレスと送信元ポートからの後続の新しい接続が、最初の接続と同じ変換関係を使用することを確認します。
- NAT アドレスとポートへの外部ホストからの新しい接続が、EIM テーブルエントリに基づいて逆アドレス変換されるようにします。

例

#NAT EIM テーブルエントリの情報を表示します。

<Sysname> display nat eim

Slot 0:

Local IP/port: 192.168.100.100/1024

Global IP/port: 200.100.1.100/2048

DS-Lite tunnel peer: -

Local VPN: vpn1

Global VPN: vpn2

Protocol: TCP(6)

Local IP/port: 192.168.100.200/2048

Global IP/port: 200.100.1.200/4096

DS-Lite tunnel peer: -

Protocol: UDP(17)

Total entries found: 2

#プロトコルが TCP である NAT EIM テーブルエントリの情報を表示します。

<Sysname> display nat eim protocol tcp

Slot: 0

Local IP/port: 192.168.100.100/1024

Global IP/port: 200.100.1.100/2048

DS-Lite tunnel peer: -

Local VPN: vpn1

Global VPN: vpn2

Protocol: TCP(6)

Total entries found: 1

表 21-4 display nat eim コマンドの表示情報の説明

フィールド	説明
CPU	CPU番号
DS-Lite tunnel peer	DS-Lite B4側トンネルアドレス。セッションがDS-Liteトンネルに属していない場合、このフィールドには 「-」 と表示されます。

フィールド	説明
Local VPN	イントラネットアドレスが属するMPLS L3VPNのVPNインスタンス名。VPNインスタンスに属していない場合、このフィールドは表示されません。
Global VPN	外部ネットワークアドレスが属するMPLS L3VPNのVPNインスタンス名。VPNインスタンスに属していない場合、このフィールドは表示されません。
Protocol	基本契約名および基本契約番号
Total entries found	現在検索されているEIMテーブルエントリの数

関連コマンド

- **nat mapping-behavior**
- **nat outbound**

関連コマンド

- **nat mapping-behavior**

21.1.7 display nat inbound

Syntax

display nat inbound

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat inbound コマンドは、NAT のインバウンドダイナミックアドレス変換の設定情報を表示します。

例

#NAT 入力インタフェースのダイナミックアドレス変換の設定情報を表示します。

```
<Sysname> display nat inbound
NAT inbound information:
  Totally 2 NAT inbound rules.
  Interface: GigabitEthernet1/0/2
    ACL: 2038          Address group: 2        Add route: Y
    NO-PAT: Y          Reversible: N
```

VPN instance: vpn1

Rule name: ruleinbound1

Priority: 1000

Config status: Active

Interface: GigabitEthernet1/0/3

ACL: 2037 Address group: 1 Add route: Y

NO-PAT: Y Reversible: N

VPN instance: vpn2

Rule name: ruleinbound2

Priority: 1000

Config status: Inactive

Reasons for inactive status:

The following items don't exist or aren't effective: local VPN, and ACL.

表 21-5 display nat inbound コマンドの表示情報の説明

フィールド	説明
NAT inbound information	NATインバウンドダイナミックアドレス変換の設定情報
Totally n NAT inbound rules	現在n個の入力方向ダイナミックアドレス変換設定があります
Interface	インバウンドダイナミックアドレス変換が設定されているインタフェース
ACL	参照先のACL番号または名前
Address group	インバウンド動的アドレス変換に使用されるアドレスグループ
Add route	ルートを追加するかどうか。値が 「Y」 の場合は、インタフェースの動的アドレス変換設定にヒットするメッセージがあると、デバイスは自動的にルートを追加します。値が 「N」 の場合は追加されません。
NO-PAT	アドレス変換にNO-PATを使用するかどうか。値がYの場合、NO-PATが使用されます。その値が “N” であれば、 PAT 方式を用いることを意味する.
Reversible	逆アドレス変換を許可するかどうか。値がYであれば、ある方向からの接続がアドレス変換テーブルエントリを正常に確立した場合に、逆方向からの接続が確立されたアドレス変換テーブルエントリを使用してアドレス変換を行うことを許可する;値が 「N」 の場合、許可されません
VPN instance	アドレスグループが属するMPLS L3VPNのVPNインスタンス名。VPNインスタンスに属していない場合、このフィールドは表示されません。
Rule name	NATルールの名前
Priority	NATルールの一致の優先順位

フィールド	説明
Config status	NAT構成のステータスの表示 • Active:有効 • Inactive:無効
Reasons for inactive status	Config statusフィールドがInactiveの場合、NATインバウンドダイナミックアドレス変換の設定が有効でない理由を示します。 • The following items don't exist or aren't effective:local VPN, address group, and ACL:構成内のアドレスグループが属する VPN インスタンス、アドレスグループ、ACL が存在しないか、有効ではありません

関連コマンド

- **nat inbound**

関連コマンド

- **nat instance**

21.1.8 display nat log

Syntax

display nat log

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

NAT ログ機能の設定情報を表示するには、**display nat log** コマンドを使用します。

例

#NAT ログ機能の設定情報を表示します。

<Sysname> display nat log

NAT logging:

Log enable : Enabled

Flow-begin :Disabled
Flow-end :Disabled
Flow-active :Disabled
Port-block-assign :Disabled
Port-block-withdraw :Disabled
Port-alloc-fail :Enabled
Port-block-alloc-fail :Disabled
Port-usage :Disabled
Port-block-usage :Enabled(40%)

表 21-6 display nat log コマンドの表示情報の説明

フィールド	説明
NAT logging	NATログ機能の設定情報
Log enable	NATログスイッチ • Enabled:オンであることを示します。ACL が指定されている場合は、指定された ACL 番号または名前が表示されます。 • Disabled:がオフであることを示します。
Flow-begin	NATセッションの新しいログ機能スイッチ • Enabled:オンであることを示します。 • Disabled:がオフであることを示します。
Flow-end	NATセッション削除ログ機能スイッチ • Enabled:オンであることを示します。 • Disabled:がオフであることを示します。
Flow-active	NATアクティブフローログ機能スイッチ • Enabled:オンであることを示します。この状態では、アクティブなフローログを生成するために設定された間隔(単位は分)が表示されます。 • Disabled:がオフであることを示します。
Port-block-assign	ポートブロック割り当てのためのNATユーザログ機能スイッチ • Enabled:オンであることを示します。 • Disabled:がオフであることを示します。
Port-block-withdraw	ポートブロック再利用のためのNATユーザログ機能スイッチ • Enabled:オンであることを示します。 • Disabled:がオフであることを示します。

フィールド	説明
Port-alloc-fail	ポート割り当て失敗のログ機能スイッチ • Enabled:オンであることを示します。 • Disabled:がオフであることを示します。
Port-block-alloc-fail	ポートブロック割り当て失敗のログ機能スイッチ • Enabled:オンであることを示します。 • Disabled:がオフであることを示します。
Port-usage	ポートブロック内のポート使用率のログ機能スイッチ • Enabled:オンであることを示します。この状態では、設定されているポート使用率のしきい値(単位:パーセント)も表示されます。 • Disabled:がオフであることを示します。
Port-block-usage	ポートブロック使用率のログ機能はオン(Enabled)で、構成済みのポートブロック使用率のしきい値(単位:パーセント)が表示されます。デフォルトは90%です。

関連コマンド

- **nat log enable**
- **nat log flow-active**
- **nat log flow-begin**

21.1.9 display nat no-pat

Syntax

display nat no-pat

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat no-pat コマンドは、NAT NO-PAT テーブルエントリ情報を表示します。

NO-PAT 動的に割り当てられる 1 対 1 のアドレスマッピング関係を記録するテーブルエントリには、次の 2 つの役割があります。

- 後続の同じ方向の新しい接続が最初の接続と同じアドレス変換関係を使用することを確認します。
- 逆方向の新しい接続は、NO-PAT テーブルを使用してアドレス変換できます。

nat inbound および nat outbound に設定された NO-PAT モードでは、メッセージアドレスを変換した後に NO-PAT テーブルを作成する必要があります。この 2 つの構成では、NO-PAT テーブルタイプが異なり、相互に使用できないため、2 つのカテゴリに分けて表示されます。

例

#NAT NO-PAT テーブルエントリを表示します。

<Sysname> display nat no-pat
Global IP: 200.100.1.100
Local IP: 192.168.100.100
Global VPN: vpn2
Local VPN: vpn1
Reversible: N
Type : Inbound

Local IP: 192.168.100.200
Global IP: 200.100.1.200
Reversible: Y
Type : Outbound

Total entries found: 2

表 21-7 display nat no-pat コマンドの表示情報の説明

フィールド	説明
CPU	CPU番号
Local VPN	イントラネットアドレスが属するMPLS L3VPNのインスタンス名。VPNインスタンスに属していない場合、この行は表示されません。
Global VPN	エクストラネットアドレスが属するMPLS L3VPNのインスタンス名。VPNインスタンスに属していない場合、この行は表示されません。
Reversible	逆アドレス変換を許可するかどうか。値がYであれば、ある方向からの接続がアドレス変換テーブルエントリを正常に確立した場合に、逆方向からの接続が確立されたアドレス変換テーブルエントリを使用してアドレス変換を行うことを許可する;値が 「N」 の場合、許可されません。

フィールド	説明
Type	NO-PATテーブルエントリタイプ • Inbound:インバウンド動的アドレス変換中に作成された NO-PAT テーブルエントリ • Outbound:出力動的アドレス変換中に作成された NO-PAT テーブルエントリ
Total entries found	現在見つかっているNO-PATテーブルエントリの数

関連コマンド

- **nat inbound**
- **nat outbound**

21.1.10 display nat outbound

Syntax

display nat outbound

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat outbound コマンドは、ダイナミックアドレス変換の設定情報を表示します。

例

#ダイナミックアドレス変換の設定情報を表示します。

<Sysname> display nat outbound

NAT outbound information:

Totally 2 NAT outbound rules.

Interface: GigabitEthernet1/0/1

ACL: 2036 Address group: 1 Port-preserved: Y

NO-PAT: N Reversible: N

Rule name: ruleoutbound1

Priority: 1000

Config status: Active

Interface: GigabitEthernet1/0/1

```
ACL: 2037          Address group: ---      Port-preserved: N
NO-PAT: Y          Reversible: Y
VPN instance: vpn_nat
Rule name: ruleoutbound2
Priority: 1000
Config status: Inactive
Reasons for inactive status:
  The following items don't exist or aren't effective: global VPN, and ACL
```

表 21-8 display nat outbound コマンドの表示情報の説明

フィールド	説明
NAT outbound information	送信方向動的アドレス変換の配置情報
Totally n NAT outbound rules	現在n個の出力動的アドレス変換が存在します
Interface	出力ダイナミックアドレス変換が設定されているインタフェース
ACL	参照先のIPv4 ACL番号または名前。構成されていない場合は、「---」と表示されます。
Address group	動的アドレス変換に使用するアドレスの組を出力する。構成されていない場合は、「---」と表示されます。
Port-preserved	PAT方式でポートを変換しないようにするかどうか
NO-PAT	変換にNO-PATを使用するかどうか。その値が“N”であれば、 PAT方式を用いることを意味する.
Reversible	逆アドレス変換を許可するかどうか。値がYであれば、ある方向からの接続がアドレス変換テーブルエントリを正常に確立した場合に、逆方向からの接続が確立されたアドレス変換テーブルエントリを使用してアドレス変換を行うことを許可する;値が 「N」 の場合、許可されません。
VPN instance	アドレスグループが属するMPLS L3VPNのVPNインスタンス名。VPNインスタンスに属していない場合、このフィールドは表示されません。
Rule name	NATルールの名前
Priority	NATルールの一致の優先順位
Config status	構成のステータスの表示 • Active:有効 • Inactive:無効

フィールド	説明
Reasons for inactive status	Config statusフィールドがInactiveの場合は、設定が有効でない理由が表示されます。 • The following items don't exist or aren't effective:global VPN, interface IP address, address group, and ACL:構成内のアドレスグループが属する VPN インスタンス、インタフェースアドレス、アドレスグループ、ACL が存在しないか、有効ではありません。 • NAT address conflicts:NAT アドレスの競合

関連コマンド

- **nat outbound**

21.1.11 display nat outbound port-block-group

Syntax

display nat outbound port-block-group

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

NAT ポートブロックのスタティックマッピングの設定情報を表示するには、**display nat outbound port-block-group** コマンドを使用します。

例

#NAT ポートブロックのスタティックマッピングの設定情報を表示します。

<Sysname> display nat outbound port-block-group

NAT outbound port block group information:

Totally 2 outbound port block group items.

Interface: GigabitEthernet1/0/2

port-block-group: 2

Rule name: rule1

Config status : Active

Interface: GigabitEthernet1/0/2
port-block-group: 10
Rule name: rule2
Config status : Inactive
Reasons for inactive status:
The following items don't exist or aren't effective: port block group.

表 21-9 display nat outbound port-block-group コマンドの表示情報の説明

フィールド	説明
NAT outbound port block group information	NATポートブロックスタティックマッピングの設定情報
Totally n outbound port block group items	現在n個のNATポートブロックのスタティックマッピング設定が存在します
Interface	NATポートブロックスタティックマッピングが設定されているインタフェース
port-block-group	ポートブロックグループ番号
Rule name	NATルールの名前
Config status	構成のステータスの表示 • Active:有効 • Inactive:無効
Reasons for inactive status	Config statusフィールドがInactiveの場合は、設定が有効でない理由が表示されます。 • The following items don't exist or aren't effective:port block group:構成内のポートブロックグループが存在しないか、有効ではありません

関連コマンド

- **nat outbound port-block-group**

21.1.12 display nat port-block

Syntax

display nat port-block { **dynamic** | **static** }[**ip** *ipv4-source-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin
network-operator

パラメータ

dynamic:動的ポートブロックテーブルエントリを表示します。

static:静的ポートブロックテーブルエントリを表示します。

ip *ipv4-source-address*:指定された IPv 4 送信元アドレスのポートブロックテーブルエントリを表示します。ipv4-source-address は、ポートブロックテーブルエントリを作成するメッセージの送信元アドレスである必要がある送信元アドレスです。

verbose:シングルボードのポートブロックテーブルエントリの詳細を表示します。構成されていない場合は、ポート・ブロック・テーブル・エントリのサマリー情報が表示されます。

説明

display nat port-block コマンドは、ポートブロックテーブルエントリを表示します。

例

#静的ポートブロックテーブルエントリを表示します。

<Sysname> display nat port-block static

Slot 0:

Local VPN	Local IP	Global IP	Port block	Connections	Extend
---	100.100.100.111	202.202.100.101	10001-10256	0	---
---	100.100.100.112	202.202.100.101	10257-10512	0	---
---	100.100.100.113	202.202.100.101	10513-10768	0	---
vpn012345678	100.100.100.113	202.202.100.101	10769-11024	0	---
901234567890					
1234567					
---	100.100.100.114	0.0.0.0	---	0	---

Total mappings found: 5

#動的ポートブロックテーブルエントリを表示します。

<Sysname> display nat port-block dynamic

Slot 0:

Local VPN	Local IP	Global IP	Port block	Connections	Extend
---	101.1.1.12	192.168.135.201	10001-11024	1	---

Total mappings found: 1

#ダイナミックポートブロックテーブルエントリの詳細を表示します。

<Sysname> display nat port-block dynamic verbose

Slot 0:

Dynamic port block entry

Local IP : 10.15.1.20

Local vpn : ---(0)

Global IP : 30.1.1.117

Global vpn : ---(0)

Port block : 1-1000

Connections : 1
FailgroupID : 1
PortLimit TCP : N/A
PortLimit UDP : N/A
PortLimit ICMP : N/A
PortLimit total : N/A
PortUsed TCP : 0
PortUsed UDP : 1
PortUsed ICMP : 0
PortUsed total : 1
Extend port block: N

Total mappings found: 1

#静的ポートブロックテーブルエントリの詳細を表示します。

<Sysname> display nat port-block static verbose

Slot 0:
Static port block entry
Local IP : 10.15.1.20
Local vpn : ---(0)
Global IP : 30.1.1.117
Global vpn : ---(0)
Port block : 1-1000
Connections : 1
FailgroupID : 1
PortLimit TCP : N/A
PortLimit UDP : N/A
PortLimit ICMP : N/A
PortLimit total : N/A
PortUsed TCP : 0
PortUsed UDP : 1
PortUsed ICMP : 0
PortUsed total : 1
Extend port block: N

Total mappings found: 1

表 21-10 display nat port-block コマンドの表示情報の説明

フィールド	説明
Local VPN	プライベートIPアドレスがVPNインスタンスに属しています。「---」は、どのVPNインスタンスにも属していないことを意味します。
Local IP	プライベートIPアドレス

フィールド	説明
Global IP	パブリックIPアドレス。0.0.0.0と表示されている場合は、パブリック・ネットワーク・リソースが不足しており、パブリックIPアドレスを割り当てることができません。
Port block	ポートブロック(開始ポート-終了ポート)。パブリック・ネットワーク・リソースが不足している場合、このフィールドは「---」と表示されます。
Connections	このポートブロック内のポートを使用して現在確立されている接続の数
Extend	インクリメンタルポートブロック数。構成されていない場合は、「---」と表示されます。
Total mappings found	現在検出されているポートブロックテーブルエントリの数

表 21-11 display nat port-block verbose コマンドの詳細表示の説明

フィールド	説明
Local IP	プライベートIPアドレス
Local vpn	プライベートIPアドレスがVPNインスタンスに属しています。「--- (0)」は、どのVPNインスタンスにも属していないことを意味します。
Global IP	パブリックIPアドレス。0.0.0.0と表示されている場合は、パブリック・ネットワーク・リソースが不足しており、パブリックIPアドレスを割り当てることができません。
Global vpn	パブリックIPアドレスがVPNインスタンスに属しています。「--- (0)」は、どのVPNインスタンスにも属していないことを示します。
Port block	ポートブロック(開始ポート-終了ポート)。パブリック・ネットワーク・リソースが不足している場合、このフィールドは「---」と表示されます。
Connections	このポートブロック内のポートを使用して現在確立されている接続の数
PortLimit TCP	TCPプロトコルに割り当てることができるポートの最大数
PortLimit UDP	UDPプロトコルに割り当てることができるポートの最大数
PortLimit ICMP	ICMPプロトコルに割り当て可能なポートの最大数
PortLimit total	最大割り当て可能ポート数
PortUsedTCP	TCPメッセージに割り当てられたポート数

フィールド	説明
PortUsedUDP	UDPメッセージに割り当てられたポート数
PortUsedICMP	ICMPメッセージに割り当てられたポート数
PortUsedtotal	割り当てられたポートの合計数
Extend port block	インクリメンタルポートブロック数。構成されていない場合は 「N」
Total mappings found	現在検出されているポートブロックテーブルエントリの数

21.1.13 display nat port-block-group

Syntax

display nat port-block-group [*group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id:ポートブロックグループの番号。範囲は 0~65535 です。この値を設定しない場合は、すべてのポートブロックグループの構成情報が表示されます。

説明

display nat port-block-group コマンドを使用して、NAT ポートブロックグループの構成情報を表示します。

例

#すべてのポートブロックグループの構成情報を表示します。

<Sysname> display nat port-block-group
NAT port block group information:
Totally 3 NAT port block groups.
Port block group 1:
Port range: 1-65535
Block size: 256
Local IP address information:

Start address	End address	VPN instance
172.16.1.1	172.16.1.254	---
192.168.1.1	192.168.1.254	vpna

```
    192.168.3.1          192.168.3.254          vpna
  Global IP pool information:
    Start address        End address
    201.1.1.1            201.1.1.10
    201.1.1.21           201.1.1.25

Port block group 2:
  Port range: 10001-30000
  Block size: 500
  Local IP address information:
    Start address        End address            VPN instance
    10.1.1.1             10.1.10.255            vpnb
  Global IP pool information:
    Start address        End address
    202.10.10.101        202.10.10.120

Port block group 3:
  Port range: 1-65535
  Block size: 256
  Local IP address information:
    Start address        End address            VPN instance
    ---                  ---                    ---
  Global IP pool information:
    Start address        End address
    ---                  ---
```

#ポートブロックグループ 1 の構成情報を表示します。

```
<Sysname> display nat port-block-group 1
  Port block group 1:
    Port range: 1-65535
    Block size: 256
    Local IP address information:
      Start address        End address            VPN instance
      172.16.1.1           172.16.1.254           ---
      192.168.1.1          192.168.1.254          vpna
      192.168.3.1          192.168.3.254          vpna
    Global IP pool information:
      Start address        End address
      201.1.1.1            201.1.1.10
      201.1.1.21           201.1.1.25
```

表 21-12 display nat port-block-group コマンドの表示情報の説明

フィールド	説明
NAT port block group information	NATポートブロックグループ情報
Totally n NAT port block groups	現在n個のポートブロックグループがあります
Port block group	ポートブロックグループの番号
Port range	パブリックアドレスのポート範囲
Block size	ポートブロックサイズ
Local IP address information	プライベートIPアドレスのメンバ情報
Global IP pool information	パブリックIPアドレスのメンバ情報
Start address	プライベート/パブリックIPアドレスメンバの開始IPアドレス。構成されていない場合は、「---」と表示されます。
End address	プライベート/パブリックIPアドレスメンバのメンバ終了IPアドレス。構成されていない場合は、「---」と表示されます。
VPN instance	プライベートIPアドレスのメンバが属するVPNインスタンス。構成されていない場合は、「---」と表示されます。

関連コマンド

- **nat port-block-group**

21.1.14 display nat server

Syntax

display nat server

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

NAT 内部サーバの設定情報を表示するには、**display nat server** コマンドを使用します。

例

#NAT 内部サーバの情報を表示します。

<Sysname> display nat server

```
NAT internal server information:
  Totally 5 internal servers.
  Interface: GigabitEthernet1/0/1
    Global ACL      : 2000
    Local IP/port : 192.168.10.1/23
    Rule name       : rule1
    Priority        : 1000
    Config status : Active

  Interface: GigabitEthernet1/0/3
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23
    Local IP/port : 192.168.10.15/23
    Rule name       : rule2
    Config status : Active

  Interface: GigabitEthernet1/0/4
    Protocol: 6(TCP)
    Global IP/port: 50.1.1.1/23-30
    Local IP/port : 192.168.10.15-192.168.10.22/23
    Global VPN      : vpn1
    Local VPN       : vpn3
    Rule name       : rule3
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN.

  Interface: GigabitEthernet1/0/4
    Protocol: 255(Reserved)
    Global IP/port: 50.1.1.100/---
    Local IP/port : 192.168.10.150/---
    Global VPN      : vpn2
    Local VPN       : vpn4
    Rule name       : rule4
    Config status : Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: interface IP address.

  Interface: GigabitEthernet1/0/5
    Protocol: 17(UDP)
    Global IP/port: 50.1.1.2/23
    Local IP/port : server group 1
                    1.1.1.1/21              (Connections: 10)
```

```
                192.168.100.200/80      (Connections: 20)
  Global VPN      : vpn1
  Local VPN       : vpn3
  Rule name       : rule5
  Config status : Active

NAT Instance: instance1
  Protocol: 6(TCP)
  Global IP/port: 1.1.1.1/0
  Local IP/port : 2.2.2.2/0
  Config status : Active
```

表 21-13 display nat server コマンドの表示情報の説明

フィールド	説明
NAT internal server information	NAT内部サーバの構成情報
Totally n internal servers	現在n個の内部サーバ構成が存在します
Interface	内部サーバ構成が存在するインタフェース
NAT Instance	内部サーバ構成が存在するNATインスタンス
Protocol	内部サーバのプロトコル番号とプロトコル名
Global IP/port	内部サーバの外部ネットワークアドレス/ポート番号 • Global IP は、単一のアドレスまたは連続したアドレスのいずれかです。Easy IP を使用している場合は、ここに指定されたインタフェースのアドレスが表示されます。インタフェースでアドレスが設定されていない場合、Global IP は「---」と表示されます。 • port は、1 つのポートにすることも、連続したポートセグメントにすることもできます。指定されたプロトコルにポートの概念がない場合、port は「---」と表示されます。

フィールド	説明
Local IP/port	通常の内部サーバの場合は、サーバのイントラネットアドレス/ポート番号を表示します。 • Local IP は、1 つのアドレスまたは連続したアドレスのいずれかです。 • port は、1 つのポートにすることも、連続したポートセグメントにすることもできます。指定されたプロトコルにポートの概念がない場合、port は「---」と表示されます。 負荷分散内部サーバの場合は、内部サーバグループ番号、サーバグループメンバのIPアドレス、ポート、接続数が表示されます。
Global VPN	外部ネットワークアドレスが属するMPLS L3VPNのVPNインスタンス名。VPNインスタンスに属していない場合、このフィールドは表示されません。
Local VPN	イントラネットアドレスが属するMPLS L3VPNのVPNインスタンス名。VPNインスタンスに属していない場合、このフィールドは表示されません。
ACL	参照先のACL番号または名前。構成されていない場合、このフィールドは表示されません。
Rule name	NATルールの名前
Priority	NATルールの一致の優先順位
Config status	構成のステータスの表示 • Active:有効 • Inactive:無効
Reasons for inactive status	Config statusフィールドがInactiveの場合は、設定が有効でない理由が表示されます。 • The following items don't exist or aren't effective:local VPN, global VPN, interface IP address, server group, and ACL: イントラネットアドレスが属する VPN インスタンス、アウトトラネットアドレスが属する VPN インスタンス、インタフェースアドレス、サーバグループ、ACL が存在しないか、有効でない設定 • Server configuration conflicts:NAT 内部サーバ構成の競合 • NAT address conflicts:NAT アドレスの競合

関連コマンド

- **nat server**

21.1.15 display nat server-group

Syntax

display nat server-group [*group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id:NAT 内部サーバグループの番号。範囲は 0~65535 です。このパラメータを指定しない場合は、すべての内部サーバグループが表示されます。

説明

NAT 内部サーバグループの設定情報を表示するには、**display nat server-group** コマンドを使用します。

例

#すべての NAT 内部サーバグループの設定情報を表示します。

<Sysname> display nat server-group

NAT server group information:

Totally 3 NAT server groups.

Group Number	Inside IP	Port	Weight
1	192.168.0.26	23	100
	192.168.0.27	23	500
2	---	---	---
3	192.168.0.26	69	100

#NAT 内部サーバグループを指定する設定情報を表示します。

<Sysname> display nat server-group 1

Group Number	Inside IP	Port	Weight
1	192.168.0.26	23	100
	192.168.0.27	23	500

表 21-14 display nat server-group コマンドの表示情報の説明

フィールド	説明
NAT server group information	NAT内部サーバグループ情報
Totally n NAT server groups	現在n個の内部サーバグループ
Group Number	内部サーバグループの番号

フィールド	説明
Inside IP	イントラネットの内部サーバグループメンバのIPアドレス。構成されていない場合は、「---」と表示されます。
Port	内部サーバグループメンバは、内部ネットワークのポートにあります。構成されていない場合は、「---」と表示されます。
Weight	内部サーバグループメンバの重み。構成されていない場合は、「---」と表示されます。

関連コマンド

- **nat server-group**

21.1.16 display nat session

Syntax

display nat session [{ **source-ip** *source-ip* | **destination-ip** *destination-ip* } *] [**brief** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

source-ip *source-ip*:指定した送信元アドレスのセッションを表示します。source-ip は、セッションを作成するメッセージの送信元アドレスである必要がある送信元アドレスです。

destination-ip *destination-ip*:指定された宛先アドレスのセッションを表示します。destination-ip は、セッションを作成するメッセージの宛先アドレスである必要がある宛先アドレスを表します。

brief:NAT セッションの概要を表示します。

verbose:NAT セッションの詳細を表示します。構成されていない場合は、セッションのサマリー情報が表示されます。

説明

display nat session コマンドは、NAT アドレス変換処理された NAT セッションを表示します。

パラメータを指定しない場合は、すべての NAT セッションの詳細が表示されます。

例

#NAT セッションの詳細を表示します。

<Sysname> display nat session verbose

```
Initiator:
  Source          IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/1
Responder:
  Source          IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.10/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet1/0/2
State: TCP_SYN_SENT
Application: SSH
Start time: 2019-07-29 19:12:36
Initiator->Responder:          1 packets          48 bytes
Responder->Initiator:          0 packets           0 bytes

Total sessions found: 1
```

#NAT セッションの簡単な情報を表示します。

<Sysname> display nat session brief

```
Slot 0:
Protocol    Source IP/port        Destination IP/port     Global IP/port
TCP          10.2.1.58/2477        20.1.1.2/1025           30.2.4.9/226
Total sessions found: 1
```

表 21-15 display nat session コマンドの表示情報の説明

フィールド	説明
CPU	CPU番号
Source IP/port	ソースIPアドレス/ポート番号
Destination IP/port	宛先IPアドレス/ポート番号
DS-Lite tunnel peer	DS-Liteトンネルのピアアドレス。セッションがDS-Liteトンネルに属していない場合、このフィールドには 「-」と表示されます。

フィールド	説明
VPN instance/VLAN ID/VLL ID	セッションが属するMPLS L3VPN/ 2層転送時セッションが属するVLAN ID/ 2層転送時セッションが属するINLINE。指定されていない場合は「-/-/-」
Protocol	DCCP、ICMP、Raw IP 、SCTP、TCP、UDP、UDP-Liteなどのトランスポート層プロトコルタイプ
Inbound interface	メッセージの受信インタフェース
State	セッション状態
Application	FTP、DNSなどを含むアプリケーション層プロトコルタイプ。OTHERは不明なプロトコルタイプを表し、対応するポートは不明なポートです。
Start time	セッション作成時間
TTL	セッションの残りの存続可能時間 (秒)
Initiator->Responder	イニシエータからレスポンダへのメッセージ数、メッセージ文節数
Responder->Initiator	レスポンダからイニシエータまでのメッセージ数、メッセージ文節数
Total sessions found	現在検出されているセッションの合計数
Source IP/port	イニシエータの送信元IPアドレス/ポート番号
Destination IP/port	イニシエータの宛先IPアドレス/ポート番号
Global IP/port	パブリックIPアドレス/ポート番号

関連コマンド

- **reset nat session**

21.1.17 display nat static

Syntax

display nat static

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

NAT スタティックアドレス変換の設定情報を表示するには、**display nat static** コマンドを使用します。

例

#NAT スタティックアドレス変換の設定情報を表示します。

<Sysname> display nat static

Static NAT mappings:

Totally 2 inbound static NAT mappings.

Net-to-net:

Global IP : 1.1.1.1 - 1.1.1.255
Local IP : 2.2.2.0
Netmask : 255.255.255.0
Global VPN : vpn2
Local VPN : vpn1
ACL : 2000
Reversible : Y
Rule name : rulenettonet
Priority : 1000
Config status: Active

IP-to-IP:

Global IP : 5.5.5.5
Local IP : 4.4.4.4
Global VPN : vpn2
Local VPN : vpn1
ACL : 2000
Reversible : Y
Rule name : ruleiptoip
Priority : 1000
Config status: Inactive
Reasons for inactive status:
The following items don't exist or aren't effective: local VPN, global VPN, and ACL.

Totally 2 outbound static NAT mappings.

Net-to-net:

Local IP : 1.1.1.1 - 1.1.1.255
Global IP : 2.2.2.0
Netmask : 255.255.255.0
Local VPN : vpn1
Global VPN : vpn2
ACL : 2000
Reversible : Y
Rule name : ruleout1
Priority : 1000
Config status: Active

```
IP-to-IP:
  Local IP       : 4.4.4.4
  Global IP      : 5.5.5.5
  Local VPN      : vpn1
  Global VPN     : vpn2
  ACL:           : 2001
  Reversible     : Y
  Rule name      : ruleout2
  Priority       : 1000
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: local VPN, and global VPN.

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: GigabitEthernet1/0/2
    Config status: Active

  Interface: GigabitEthernet1/0/3
    Config status: Active
```

表 21-16 display nat static コマンドの表示情報の説明

フィールド	説明
Static NAT mappings	静的アドレス変換の構成情報
Totally n inbound static NAT mappings	現在n個の入力方向静的アドレス変換の構成が存在する
Totally n outbound static NAT mappings	現在n個の出力方向の静的アドレス変換が存在する構成
Net-to-net	ネットワークセグメント間の静的アドレス変換マッピング
IP-to-IP	IPからIPへの静的アドレス変換マッピング
Local IP	イントラネットIPアドレスまたはアドレス範囲
Global IP	外部IPアドレスまたはアドレス範囲
Netmask	IPアドレスマスク
Local VPN	イントラネットアドレスが属するMPLS L3VPNのVPNインスタンス名。VPNインスタンスに属していない場合、このフィールドは表示されません。
Global VPN	外部ネットワークアドレスが属するMPLS L3VPNのVPNインスタンス名。VPNインスタンスに属していない場合、このフィールドは表示されません。

フィールド	説明
ACL	参照先のACL番号または名前。構成されていない場合、このフィールドは表示されません。
Reversible	逆アドレス変換を許可するかどうか。値がYであれば、ある方向からの接続がアドレス変換テーブルエントリを正常に確立した場合に、逆方向からの接続が確立されたアドレス変換テーブルエントリを使用してアドレス変換を行うことを許可する 構成されていない場合、このフィールドは表示されません。
Interfaces enabled with static NAT	静的アドレス変換がインタフェースでオンになっている場合
Totally n interfaces enabled with static NAT	現在n個のインタフェースが静的アドレス変換を有効にしている
Interface	静的アドレス変換機能を有効にするインタフェース
Rule name	NATルールの名前
Priority	NATルールの一致の優先順位
Config status	構成のステータスの表示 • Active:有効 • Inactive:無効
Reasons for inactive status	Config statusフィールドがInactiveの場合は、設定が有効でない理由が表示されます。 • The following items don't exist or aren't effective:local VPN, global VPN, and ACL:設定内のイントラネットアドレスが属する VPN インスタンス、アウトトラネットアドレスが属する VPN インスタンス、ACL が存在しない、または存在しない • NAT address conflicts:NAT アドレスの競合

関連コマンド

- **nat static**
- **nat static net-to-net**
- **nat static enable**

21.1.18 display nat statistics

Syntax

display nat statistics [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

summary:NAT 統計の要約情報を表示します。このパラメータを指定しない場合は、NAT 統計の詳細が表示されます。

説明

NAT 統計を表示するには、**display nat statistics** コマンドを使用します。

例

#すべての NAT 統計の詳細を表示します。

<Sysname> display nat statistics

```
Slot 1:
  Total session entries: 100
  Total EIM entries: 1
  Total inbound NO-PAT entries: 0
  Total outbound NO-PAT entries: 0
  Total static port block entries: 10
  Total dynamic port block entries: 15
  Active static port block entries: 0
  Active dynamic port block entries: 0
```

表 21-17 display nat statistics コマンドの表示情報の説明

フィールド	説明
Total session entries	NATセッションテーブルエントリ数
Total EIM entries	EIMテーブル・アイテム数
Total inbound NO-PAT entries	入力方向のNO-PATテーブルエントリ数
Total outbound NO-PAT entries	出力方向のNO-PATテーブルエントリ数
Total static port block entries	現在の構成で作成された静的ポートブロックテーブルエントリの数
Total dynamic port block entries	現在の構成で作成可能な動的ポート・ブロック・テーブル・エントリの数。割り当てられたポートブロックと割り当てられていないポートブロックを含む、割り当て可能な動的ポートブロックの合計数。
Active static port block entries	現在使用されている静的ポートブロックテーブルエントリの数

フィールド	説明
Active dynamic port block entries	現在作成されているダイナミックポートブロックテーブルエントリの数、つまり割り当てられているダイナミックポートブロックの数

#すべての NAT 統計の概要を表示します。

<Sysname> display nat statistics summary

EIM: Total EIM entries.

SPB: Total static port block entries.

DPB: Total dynamic port block entries.

ASPB: Active static port block entries.

ADPB: Active dynamic port block entries.

Slot	Sessions	EIM	SPB	DPB	ASPB	ADPB
1	100	1	10	15	0	0

表 21-18 display nat statistics summary コマンドの表示情報の説明

フィールド	説明
CPU	CPU番号
Sessions	NATセッションテーブルエントリ数
EIM	EIMテーブル・アイテム数
SPB	現在の構成で作成された静的ポートブロックテーブルエントリの数
DPB	現在の構成で作成可能な動的ポート・ブロック・テーブル・エントリの数。割り当てられたポートブロックと割り当てられていないポートブロックを含む、割り当て可能な動的ポートブロックの合計数。
ASPB	現在使用されている静的ポートブロックテーブルエントリの数
ADPB	現在作成されているダイナミックポートブロックテーブルエントリの数、つまり割り当てられているダイナミックポートブロックの数

21.1.19 global-ip-pool

Syntax

global-ip-pool *start-address end-address*

undo global-ip-pool *start-address*

デフォルト

パブリックアドレスメンバは存在しません。

View

NAT port block group view

定義済みユーザロール

network-admin

パラメータ

start-address end-address:パブリックアドレスメンバの開始 IP アドレスと終了 IP アドレス。end-address は start-address 以上でなければなりません;start-address と end-address が同じ場合、アドレスは 1 つだけです。

説明

global-ip-pool コマンドは、パブリックアドレスのメンバを追加するために使用します。

undo global-ip-pool コマンドを使用して、パブリックアドレスのメンバを削除します。

NAT ポートブロックスタティックマッピングでは、ポートはパブリックアドレスメンバの IP アドレスに基づいて、プライベートアドレスメンバの IP アドレスにポートブロックを割り当てます。1 つのパブリック IP アドレスに対応できるポートブロックの数は、ポートブロックグループに構成されているパブリック IP アドレスのポート範囲とポートブロックサイズによって決まります(ポートブロックサイズで割ったポート範囲)。

1 つのポートブロックグループ内に 1 回に追加するパブリックアドレスメンバの数は 256 以下であり、パブリックアドレスメンバ間で IP アドレスを重複させることはできません。

異なるポートブロックグループ間のパブリックネットワークアドレスメンバの IP アドレスは重複できますが、アドレスが重複する場合はポート範囲が重複しないようにしてください。

パブリックアドレスのメンバが NAT ポートブロックのスタティックマップのパブリックアドレスのメンバと重複している場合は、NAT ポートブロックのスタティックマップのポート範囲と NAT ポートブロックのダイナミックマップのポート範囲が重複していないことを確認します。そうしないと、ユーザがオンラインになったときに、デバイスが同じパブリック IP アドレスとポートブロックを 2 人の異なるユーザに割り当てた場合、どちらかのユーザの NAT セッションが作成されないことがあります。

例

#IP アドレス 202.10.1.1 から 202.10.1.10 までのパブリックネットワークアドレスメンバをポートブロックグループ 1 に追加します。

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] global-ip-pool 202.10.1.1 202.10.1.10
```

関連コマンド

- **nat port-block-group**

21.1.20 inside ip

Syntax

inside ip *inside-ip* **port** *port-number* [**weight** *weight-value*]

undo inside ip *inside-ip* **port** *port-number*

デフォルト

内部サーバグループには、内部サーバグループのメンバはありません。

View

Internal server group view

定義済みユーザロール

network-admin

パラメータ

inside-ip:内部サーバグループのメンバの IP アドレス。

port *port-number*:内部サーバグループのメンバがサービスを提供するポート番号。範囲は 1~65535 (FTP データポート番号 20 以外)です。

weight *weight-value*:内部サーバグループメンバの重み。weight-value は重みです。範囲は 1~1000 で、デフォルト値は 100 です。内部サーバグループのメンバは重みの割合に応じて外部にサービスを提供し、重みの値が大きい内部サーバグループのメンバほど外部にサービスを提供する割合が大きくなる。

説明

inside ip コマンドを使用して、内部サーバグループのメンバを追加します。

undo inside ip コマンドを使用して、内部サーバグループのメンバを削除します。

例

#内部サーバグループ 1 に、IP アドレス 10.1.1.2、サービスポート番号 30 を持つ内部サーバグループメンバを追加します。

<Sysname> system-view
[Sysname] nat server-group 1
[Sysname-nat-server-group-1] inside ip 10.1.1.2 port 30

関連コマンド

- **nat server-group**

21.1.21 local-ip-address

Syntax

local-ip-address *start-address end-address*

undo local-ip-address *start-address end-address*

デフォルト

プライベートネットワークアドレスメンバは存在しません。

View

NAT port block group view

定義済みユーザロール

network-admin

パラメータ

start-address end-address:プライベートネットワークアドレスメンバの開始 IP アドレスと終了 IP アドレス。end-address は start-address 以上でなければなりません;start-address と end-address が同じ場合、アドレスは 1 つだけです。

説明

local-ip-address コマンドを使用して、プライベートネットワークアドレスのメンバを追加します。

undo local-ip-address コマンドは、プライベートネットワークアドレスメンバを削除するために使用します。

プライベートネットワークアドレスメンバの IP アドレスは、ポートブロックの利用者として、ポートブロック群に配置されたパブリックアドレスメンバの IP アドレスに基づいてポートブロックを割り当てる。1 つのポートブロックグループ内で、1 つのプライベート IP アドレスに割り当てられるポートブロックは 1 つだけです。

同じポートブロックグループ内で、複数のプライベートネットワークアドレスメンバを構成できます。

- 同じ VPN インスタンスに属するプライベートネットワークアドレスのメンバ間で IP アドレスを重複させることはできません。
- どの VPN インスタンスにも属していないプライベートネットワークアドレスのメンバ間で IP アドレスを重複させることはできません。

異なるポートブロックグループ内で、同じ VPN インスタンスを指定してこのコマンドを実行する場合は、設定されているプライベートネットワークアドレスメンバの IP アドレスが重複しないようにしてください。重複しないと、NAT トラフィックが正しく処理されない可能性があります。

ポートブロックグループ内のプライベートネットワークアドレスの合計数が、割り当て可能なポートブロックの合計数(ポートブロックサイズで割ったポート範囲)を超えると、

NAT ポートブロックのスタティックマッピング時に、超過部分のプライベートネットワークアドレスはポートブロックに割り当てられません。

例

#IP アドレスが 172.16.1.1~172.16.1.255 で、VPN インスタンスが vpn 1 であるプライベートネットワークアドレスメンバをポートブロックグループ 1 に追加します。

<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] local-ip-address 172.16.1.1 172.16.1.255 vpn-instance vpn1

関連コマンド

- **nat port-block-group**

21.1.22 nat address-group

Syntax

nat address-group *group-id*

undo nat address-group *group-id*

デフォルト

アドレスグループが存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id:アドレスグループ番号。範囲は 0~65535 です。

説明

nat address-group コマンドを使用して、アドレスグループを作成し、アドレスグループの表示を開始します。指定したアドレスグループがすでに存在する場合は、アドレスグループ表示に直接進みます。

undo nat address-group コマンドを使用して、指定したアドレスグループを削除します。

1 つのアドレスグループは複数のアドレスグループメンバの集合であり、各アドレスグループメンバは address コマンドで構成されます。

例

#1 という番号のアドレスグループを作成します。

<Sysname> system-view
[Sysname] nat address-group 1

関連コマンド

- **address**
- **display nat address-group**
- **display nat all**
- **nat inbound**
- **nat outbound**

21.1.23 nat alg

Syntax

nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

undo nat alg { **all** | **dns** | **ftp** | **h323** | **icmp-error** | **ils** | **mgcp** | **nbt** | **pptp** | **rsh** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** | **xdmcp** }

デフォルト

DNS プロトコル、FTP プロトコル、ICMP エラー制御メッセージ、PPTP プロトコル、および RTSP プロトコルの NAT ALG 機能がオンになり、他のプロトコルタイプの NAT ALG 機能がオフになります。

View

System view

定義済みユーザロール

network-admin

パラメータ

all:指定可能なすべてのプロトコルの ALG 機能。

dns:DNS プロトコルの ALG 機能を表す。

ftp:FTP プロトコルの ALG 機能を表す。

h 323:H 323 プロトコルの ALG 機能を表す。

icmp-error:ICMP 誤り制御メッセージの ALG 機能を示す。

ils:ILS (Internet Locator Service、インターネット位置情報サービス)プロトコルの ALG 機能を表す。

mgcp:MGCP (Media Gateway Control Protocol、メディアゲートウェイ制御プロトコル)プロトコルの ALG 機能を表す。

nbt:NBT (NetBIOS over TCP/IP、TCP/IP ベースのネットワーク基本入出力システム)プロトコルの ALG 機能を表す。

pptp:PPTP (Point-to-Point Tunneling Protocol 0 ポイントツーポイントトンネリングプロトコル)プロトコルの ALG 機能を表す。

rsh:RSH (Remote Shell、リモートシェル)プロトコルの ALG 機能を表す。

rtsp:RTSP (Real Time Streaming Protocol、ライブストリームプロトコル)プロトコルの ALG 機能を表す。

sccp:SCCP (Skinny Client Control Protocol、クライアント制御プロトコルの縮小)プロトコルの ALG 機能を表す。

sip:SIP (Session Initiation Protocol、セッション開始プロトコル)プロトコルの ALG 機能を表す。

sqlnet:SQLNET プロトコルの ALG 機能を表す。

tftp:TFTP プロトコルの ALG 機能を表す。

xdmcp:XDMCP (X Display Manager Control Protocol, X モニタを表示する)プロトコルの ALG 機能を表す。

説明

nat alg コマンドは、指定したプロトコルタイプまたはすべてのプロトコルタイプの NAT ALG 機能を有効にします。

undo nat alg コマンドは、指定されたプロトコルタイプまたはすべてのプロトコルタイプの NAT ALG 機能をオフにします。

ALG (Application Level Gateway、アプリケーション層ゲートウェイ)は主にアプリケーション層のメッセージの解析と処理を行う。通常、NAT では、ヘッダー内の IP アドレスとポート情報のみが変換され、アプリケーション層のデータペイロード内のフィールドは分析および処理されません。ただし、一部のアプリケーション層プロトコルでは、メッセージのデータペイロードに IP アドレスまたはポート情報が含まれている場合があります。これらのペイロード情報も有効に変換する必要があります。そうしないと、機能が低下する可能性があります。

たとえば、FTP アプリケーションは、データ接続と制御接続の両方によって実行され、データ接続が使用するアドレスとポートは、制御接続ネゴシエーションメッセージ内のロード情報によって決定されるため、後続のデータ接続が正しく確立されるように、NAT の関連する変換設定を使用してロード情報の変換を完了する必要があります。

例

#FTP プロトコルの ALG 機能を有効にします。

```
<Sysname> system-view
[Sysname] nat alg ftp
```

関連コマンド

- **display nat all**

21.1.24 nat dns-map

Syntax

nat dns-map domain *domain-name* **protocol** *pro-type* { **interface** *interface-type interface-number* | **ip** *global-ip* } **port** *global-port*

undo nat dns-map domain *domain-name*

デフォルト

内部サーバへのドメイン名マッピングがありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

domain *domain-name*:内部サーバの正当なドメイン名を指定します。domain-name は内部サーバのドメイン名で、 「.」 で区切られた文字列(例 aabbcc.com)で構成され、各文字列は 63 文字以下、 「.」 を含めた全体で 253 文字以下で構成されます。大文字と小文字は区別されず、文字列には文字、数字、 「-」 、 「_」 、または 「.」 を含めることができます。

protocol *pro-type*:内部サーバのプロトコルタイプを指定します。pro-type は特定のプロトコルタイプを表し、tcp または udp の値を取ります。

interface *interface-type interface-number*:指定されたインタフェースのアドレスを内部サーバの外部ネットワークアドレスとして使用することを示します。interface-type interface-number は、インタフェースタイプとインタフェース番号を示します。

ip *global-ip*:内部サーバが外部ネットワークアクセスに提供する IP アドレスを指定します。global-ip は、エクストラネットの IP アドレスです。

port *global-port*:内部サーバが外部ネットワークアクセスに提供するサービスポート番号を次の形式で指定します。

- 数値:1~65535 の範囲で値を指定します。
- プロトコル名:ftp、telnet などの 1~15 文字の文字列。

説明

nat dns-map コマンドは、内部サーバへのドメイン名のマッピングを設定するために使用します。

undo nat dns-map コマンドは、内部サーバへのドメイン名のマッピングを削除するために使用します。

NAT の DNS mapping 機能は内部サーバと連携する必要があり、主に DNS サーバがエクストラネットに、アプリケーションサーバがイントラネット(NAT デバイス上の対応する

nat server 設定)にあり、イントラネットのユーザがドメイン名を介してイントラネットアプリケーションサーバにアクセスする必要がある場合に適用される。エクストラネットからの DNS 応答メッセージのペイロードには、ドメイン名とアプリケーションサーバのエクストラネット IP アドレス(トランスポート・プロトコル・タイプとポート番号が含まれていない)しか含まれていないが、インタフェース上に複数の NAT サーバ構成が存在し、同じエクストラネットアドレスを使用しているのにイントラネットアドレスが異なる場合、IP アドレスのみを使用して内部サーバを照合すると誤った照合結果が得られることがある。そのため、DNS mapping の構成を利用して、ドメイン名と応用サーバの外部ネットワーク IP アドレス、ポートとプロトコルのマッピング関係を指定して、ドメイン名から応用サーバの外部ネットワーク IP アドレス、ポートとプロトコルを取得して、(現在の NAT インタフェース上)内部サーバの構成と正確に一致して、応用サーバの内部ネットワーク IP アドレスを取得する。

アプライアンスは内部サーバへの複数のドメイン名のマッピングの設定をサポートできます。

例

#ある会社は、 Web サービスを内部から外部に提供しており、内部サーバのドメイン名は www.server.com,、外部の IP アドレスは 202.112.0.1,サービスポート番号は 12345 である。社内ユーザがドメイン名を使用して社内 Web サーバにアクセスできるように、ドメイン名から社内サーバへのマッピングを設定します。

<Sysname> system-view
[Sysname] nat dns-map domain www.server.com protocol tcp ip 202.112.0.1 port 12345

関連コマンド

- **display nat all**
- **display nat dns-map**
- **nat server**

21.1.25 nat inbound

Syntax

nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** *group-id* [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*]

undo nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* }

デフォルト

インバウンドダイナミックアドレス変換設定はありません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number:ACL の番号。範囲は 2000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

address-group group-id:アドレス変換に使用するアドレスグループを指定します。group-id はアドレスグループの番号で、範囲は 0~65535 です。

no-pat:メッセージのポート情報を使わずに NO-PAT 方式で変換することを示す。本パラメータが指定されていない場合は、 PAT 方式による変換、すなわち変換時にメッセージのポート情報を使用することを意味する。PAT 方式は TCP, UDP および ICMP クエリメッセージのみをサポートし、 ICMP メッセージにはポートの概念がないため、 ICMP ID を ICMP メッセージの送信元ポートとする。

reversible:逆アドレス変換が許可されていることを示します。すなわち、イントラネットのユーザがイントラネットへの接続を積極的に開始し、アドレス変換テーブルエントリの確立に成功した場合、イントラネットがそのイントラネットのユーザへの接続を許可し、確立されたアドレス変換テーブルエントリを使用して宛先アドレス変換を行う。

add-route:変換されたアドレスにルーティングテーブルを付加し、その宛先アドレスを変換後のアドレス、出インタフェースをアドレス変換を行うインタフェース、次ホップをそのメッセージ変換前のソースアドレスとする。

rule *rule-name*:NAT ルールの名前。1~63 文字の文字列で、大文字と小文字が区別されます。「¥」 、「/」 、「:」 、「*」 、「?」 は使用できません。」 、「<」 、「>」 、「|」 、「」、 「@」 です。このパラメータを指定しない場合、名前はありません。

priority *priority*:0~2147483647 の範囲で一致する NAT ルールの優先度。値が小さいほど優先度が高くなります。このパラメータを指定しない場合、対応する NAT ルールが最も優先されます。

説明

nat inbound コマンドを使用して、インバウンドダイナミックアドレス変換を設定します。

undo nat inbound コマンドは、指定されたインバウンド動的アドレス変換を削除します。

インバウンドアドレス変換が設定されているインタフェースから受信した ACL permit 規則に準拠するメッセージは、アドレスグループ group-id のアドレスを用いてソースアドレス変換される。

インバウンドアドレス変換には 2 つの変換方法があります。

- PAT 方式:エクストラネットからイントラネットへのメッセージに対して、 ACL を満たすならば、アドレスグループ中のアドレスを用いてソースアドレス変換を行い、同時にソースポート(IP1/port1 IP2/port2 に変換)を変換する。

- NO-PAT 方式:エクストラネットからイントラネットへのメッセージは、 ACL に適合していればアドレスグループ中のアドレスを用いて発信元アドレス変換を行い、発信元ポートを変換しない(IP 1 を IP 2 に変換).;ユーザが reversible を設定している場合、IP 2 を介したイントラネットからアウトトラネットへのアクティブなアクセスが許可されます。このようなアクセスメッセージには、ACL の逆マッチングが必要です(メッセージの送信元/ポートと宛先アドレス/ポートを抽出し、宛先アドレスを IP 1 に変換してから、送信元/ポートと宛先アドレス/ポートを入れ替えて ACL に一致させます。)。ACL に逆マッチングされたメッセージのみが変換されます(宛先アドレス IP 2 を IP 1 に変換)。そうでない場合は変換されません。

nat inbound コマンドは通常、nat outbound、nat server、または nat static とともに使用され、送信元と宛先の両方の変換、つまり双方向 NAT を外部ネットワーク側のポートでサポートします。

入力方向と出力方向の動的アドレス変換で参照されるアドレスグループを指定する場合は、次の点に注意してください。

- アドレスグループが nat inbound 設定で参照されると、nat outbound 設定で参照できなくなります。
- 1 つのアドレスグループが PAT 方式の nat inbound 構成で参照されると、NO-PAT 方式の nat inbound 構成では参照できなくなり、その逆もできなくなります。

add-route パラメータは、イントラネットとアウトトラネットのアドレスが重複するネットワークシナリオには適用できません。他のメッシュシーンでは、次の操作を実行します。

- add-route パラメータが指定されている場合、構成にヒットするメッセージがあると、デバイスはルーティングテーブルエントリを自動的に追加します。
- add-route パラメータが指定されていない場合、ユーザはデバイスに手動でルートを追加する必要があります。ルーティングテーブルエントリの自動追加には時間がかかるため、通常は手動でルートを追加することをお勧めします。

1 つのインタフェースでは、ACL は 1 つの nat inbound によってのみ参照できます。

1 つのインタフェースで複数のインバウンドアドレス変換を同時に設定できる。

インバウンドダイナミックアドレス変換では、NAT ルールの一致優先順位が同じ場合、デバイスは ACL 名または ACL 番号で一致し、次のルールでは ACL 名の優先順位が ACL 番号の優先順位よりも高くなります。

- ACL 名の場合、デバイスは名前の比較結果の優先順位に従って一致します。
- ACL 番号の場合、番号が大きいほどプライオリティが高くなり、デバイスが優先的に一致します。

例

#10.110.10.0/24 ネットワークセグメントのホストのアドレス変換を許可するように ACL 2001 を設定します。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255
```

[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit

#アドレスグループ 1 を設定し、アドレスグループメンバ 202.110.10.10、202.110.10.11、202.110.10.12 を追加します。

[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit

#ダイナミックアドレス変換をインタフェース GigabitEthernet1/0/1 で設定し、アドレスグループ 1 のアドレスを使用してアドレス変換を行い、変換時に TCP/UDP のポート情報を使用せず、ルートを追加する必要があります。また、このインバウンドダイナミック NAT ルールの名前を abc、一致優先順位を 0 に指定します。

[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat inbound 2001 address-group 1 no-pat add-route rule abc priority 0

関連コマンド

- **display nat all**
- **display nat inbound**
- **display nat no-pat**

21.1.26 nat inbound rule move

Syntax

nat inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

デフォルト

インバウンドダイナミック NAT ルールの位置によって一致の優先順位が決まり、上位の NAT ルールほど一致の優先順位が高くなります。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1:移動する NAT ルールの名前。

after:nat-rule-name1 を nat-rule-name2 の後ろに移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値+1 になります。

before:nat-rule-name1 を nat-rule-name2 の前に移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値は-1 になります。

nat-rule-name2:移動する NAT ルールの名前。

説明

nat inbound rule move コマンドを使用して、インバウンドダイナミック NAT ルールの一致優先順位を調整します。

このコマンドは、NAT ルール名が指定されたインバウンドダイナミック NAT に対してのみ有効です。

前に移動された NAT ルールでは、デバイスが優先的に一致します。

例

#インタフェース GigabitEthernet1/0/1 で、インバウンドダイナミック NAT ルール abc をインバウンドダイナミック NAT ルール def の前に移動します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat inbound rule move abc before def

関連コマンド

- **nat inbound**

21.1.27 nat log enable

Syntax

nat log enable [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat log enable

デフォルト

NAT ログ機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

acl:ACL の番号または名前を指定します。

ipv4-acl-number:ACL の番号。範囲は 2000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

説明

nat log enable コマンドは、NAT ログ機能を有効にするために使用します。

undo nat log enable コマンドは、NAT ログ機能を無効にするために使用します。

NAT ログ機能を有効にするには、NAT セッションログ機能(NAT 新規セッション、NAT 削除セッション、および NAT アクティブフローのログ機能が含まれます。)、NAT ユーザログ機能(NAT ポートブロックの割り当てと NAT ポートブロックの再利用を含むログ機能)、および NAT 警告ログ機能を有効にする必要があります。

acl パラメータは、NAT セッションログ機能でのみ有効で、他の NAT ログ機能では無効です。ACL が指定されている場合、ACL permit ルールに一致するトラフィックのみが NAT セッションログの出力をトリガする可能性があります;ACL が指定されていない場合、NAT セッションログの出力は、NAT によって処理されるすべてのトラフィックでトリガされる可能性があります。

例

#NAT ログ機能を有効にします。

<Sysname> system-view
[Sysname] nat log enable

関連コマンド

- **display nat all**
- **display nat log**
- **nat log flow-active**
- **nat log flow-begin**
- **nat log flow-end**
- **nat log port-alloc-fail**
- **nat log port-block-alloc-fail**

21.1.28 nat log flow-active

Syntax

nat log flow-active *time-value*

undo nat log flow-active

デフォルト

NAT アクティブフローのログ機能はオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value:NAT アクティブフローログの出力がトリガされる間隔を分単位で 10~120 の範囲で指定します。

説明

nat log flow-active コマンドを使用して、NAT アクティブフローログ機能を有効にし、アクティブフローログを生成する間隔を設定します。

undo nat log flow-active コマンドを使用して、NAT アクティブフローのログ機能を無効にします。

長期間切断されていない NAT セッション(アクティブストリーム)の接続を定期的に記録する必要がある場合は、アクティブなフローログ機能を使用できます。

NAT アクティブフローログ機能が有効になっている場合、デバイスは、指定された時間間隔ごとに NAT アクティブフローのログを記録します。

アクティブフローログ機能は、NAT ログ機能(nat log enable コマンドを使用)がオンになっている場合にのみ有効になります。

例

#NAT アクティブフローログ機能を有効にし、NAT アクティブフローログを出力する間隔を 10 分に設定します。

<Sysname> system-view
[Sysname] nat log flow-active 10

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

21.1.29 nat log flow-begin

Syntax

nat log flow-begin

undo nat log flow-begin

デフォルト

NAT 新規セッションのログ機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

nat log flow-begin コマンドは、NAT 新規セッションのログ機能を有効にするために使用します。

undo nat log flow-begin コマンドは、NAT 新規セッションのログ機能を無効にします。

NAT ログ機能が有効になるのは、NAT ログ機能(nat log enable コマンドを使用)が有効になっている場合だけです。

例

#NAT 新規セッションのログ機能を有効にします。

<Sysname> system-view
[Sysname] nat log flow-begin

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

21.1.30 nat log flow-end

Syntax

nat log flow-end

undo nat log flow-end

デフォルト

NAT 削除セッションのログ機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

nat log flow-end コマンドは、NAT 削除セッションのログ機能を有効にします。

undo nat log flow-end コマンドを使用して、NAT 削除セッションのログ機能を無効にします。

NAT 削除セッションのログ機能は、NAT ログ機能(nat log enable コマンドを使用)が有効になっている場合にのみ有効になります。

例

#NAT 削除セッションのログ機能を有効にします。

<Sysname> system-view
[Sysname] nat log flow-end

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

21.1.31 nat log port-block usage threshold

Syntax

nat log port-block usage threshold *value*

undo nat log port-block usage threshold

デフォルト

NAT ポートブロック使用率のしきい値は 90%です。

View

System view

定義済みユーザロール

network-admin

パラメータ

value:ポートブロック使用率のしきい値。40~100 の範囲で、パーセンテージで指定します。

説明

nat log port-block usage threshold コマンドを使用して、NAT ポートブロック使用率のしきい値を設定します。

undo nat log port-block usage threshold コマンドを実行すると、デフォルトの状態に戻ります。

ポートブロックの使用率が設定された割合を超えると、ログ情報が出力されます。

このコマンドは、NAT ログ機能(nat log enable コマンドを使用)がオンになっている場合にのみ有効です。

例

#NAT ポートブロックの使用率アラームしきい値を 80%に設定します。

<Sysname> system-view

[Sysname] nat log port-block usage threshold 80

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

21.1.32 nat mapping-behavior endpoint-independent

Syntax

nat mapping-behavior endpoint-independent [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat mapping-behavior endpoint-independent

デフォルト

PAT 送信方向動的方式アドレス変換のモードは Address and Port-Dependent Mapping である。

View

System view

定義済みユーザロール

network-admin

パラメータ

acl:指定されたアドレス変換モードに準拠する必要があるメッセージ範囲を制御する ACL の番号または名前を指定します。

ipv4-acl-number:ACL の番号。範囲は 2000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

説明

nat mapping-behavior endpoint-independent コマンドは、ダイナミックアドレス変換の PAT モードを Endpoint-Independent Mapping に設定します。

undo nat mapping-behavior endpoint-independent コマンドを使用して、デフォルトの状態を復元します。

PAT 方式出力方向ダイナミックアドレス変換は 2 つのモードをサポートしています。

- Endpoint-Independent Mapping (ピアアドレスとポートの変換モードには関係ありません。):同一の送信元アドレスと送信元ポート番号からのメッセージであれば、その宛先アドレスが同一であるかどうかにかかわらず、 PAT マッピングにより、その

送信元アドレスと送信元ポート番号が同一の外部アドレスとポート番号に変換され、そのマッピング関係が記録され EIM 表エントリが生成される.;NAT ゲートウェイデバイスは、変換されたアドレスとポートを使用して、外部ネットワークのホストが内部ネットワークのホストにアクセスできるようにします。このモードは、異なる NAT ゲートウェイの背後にあるホスト間の相互アクセスをサポートします。

- Address and Port-Dependent Mapping (ピアアドレスとポートの変換モードに注意してください。):同じ送信元アドレスと送信元ポート番号からのメッセージについて、その宛先アドレスと宛先ポート番号が異なれば、同じ送信元アドレスと送信元ポート番号が同じ外部アドレスとポート番号に変換されることを要求しないため、PAT マッピングにより、同じ送信元アドレスと送信元ポート番号が異なる外部アドレスとポート番号に変換されることが多い。また、NAT ゲートウェイ・デバイスは、変換されたアドレスとポートを使用して、これらの宛先アドレスに対応する外部ネットワークのホストのみが内部ネットワークのホストにアクセスできるようにします。このモードはセキュリティは優れていますが、異なる NAT ゲートウェイの背後にあるホスト間の相互アクセスには不便です。

この配置は、出力方向動的アドレス変換の PAT 方式に対してのみ機能する。双方向ダイナミックアドレス変換の PAT 方式の変換モードは常に Address and Port-Dependent Mapping である。

acl パラメータが設定されている場合は、ACL permit ルールに一致するメッセージのみが Endpoint-Independent Mapping モードでアドレス変換されます。acl パラメータが設定されていない場合は、すべてのメッセージが Endpoint-Independent Mapping モードでアドレス変換されます。

例

#すべてのメッセージを Endpoint-Independent Mapping モードでアドレス変換する。

```
<Sysname> system-view
[Sysname] nat mapping-behavior endpoint-independent
```

#FTP および HTTP メッセージのみ Endpoint-Independent Mapping モードでアドレス変換し、その他のメッセージは Address and Port-Dependent Mapping モードでアドレス変換します。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80
[Sysname-acl-ipv4-adv-3000] rule permit tcp destination-port eq 21
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] nat mapping-behavior endpoint-independent acl 3000
```

関連コマンド

- **nat outbound**
- **display nat eim**

21.1.33 nat outbound

デフォルト

ダイナミックアドレス変換設定がありません。

Syntax

- NO-PAT モード

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] **address-group** *group-id* **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

- PAT 方式

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** *group-id*] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number:ACL の番号。範囲は 2000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

address-group *group-id*:アドレス変換に使用するアドレスグループを指定します。group-id はアドレスグループの番号で、範囲は 0~65535 です。このパラメータを指定しない場合は、変換後のアドレスとしてインタフェースの IP アドレスが直接使用され、Easy IP 機能が実装されます。

no-pat:NO-PAT 方式を用いて変換を行うこと、すなわち変換時にメッセージを用いないポート情報を示す.;本パラメータが指定されていない場合は、 PAT 方式による変換、すなわち変換時にメッセージのポート情報を使用することを意味する。PAT 方式は TCP, UDP および ICMP クエリメッセージのみをサポートし、 ICMP メッセージにはポートの概念がないため、 ICMP ID を ICMP メッセージの送信元ポートとする。

reversible:逆アドレス変換が許可されていることを示します。すなわち、イントラネットユーザが積極的にアウトトラネットに接続を開始し、アドレス変換テーブルエントリの確立に成功した場合、アウトトラネットがそのイントラネットユーザに開始した接続に対して、確立されたアドレス変換テーブルエントリを使用して宛先アドレス変換を行うことを許可する。

port-preserved:PAT 方式でポートを割り当てる場合はなるべくポートを変換しない。port-preserved パラメータは NAT ポートブロックダイナミックマッピングに無効です。

rule *rule-name*:NAT ルールの名前。1~63 文字の文字列で、大文字と小文字が区別されます。「¥」 、「/」 、「:」 、「*」 、「?」 は使用できません。」 、「<」 、「>」 、「|」 、「」、 「@」 です。このパラメータを指定しない場合、名前はありません。

priority *priority*:0~2147483647 の範囲で一致する NAT ルールの優先度。値が小さいほど優先度が高くなります。このパラメータを指定しない場合、対応する NAT ルールが最も優先されます。

説明

出力ダイナミックアドレス変換を設定するには、**nat outbound** コマンドを使用します。

undo nat outbound コマンドは、指定された出力ダイナミックアドレス変換を削除します。

一般に、出力方向動的アドレス変換は外部ネットワークに接続されたインタフェース上に配置され、 1 つのインタフェースで複数の出力方向アドレス変換を同時に配置することができる。動的アドレス変換には、次の 2 つの方法があります。

- PAT 方式:イントラネットからアウトトラネットへのメッセージに対して、 ACL permit ルールに適合していれば、アドレスグループ中のアドレスあるいはそのインタフェースのアドレス(Easy IP 方式)を用いてソースアドレス変換を行い、同時にソースポート(IP1/port1 IP2/port2 に変換)を変換する.;PAT 方式でのアドレス変換モードを EIM (Endpoint-Independent Mapping)にも設定しておけば、エクストラネットは IP2/port2 を介してイントラネットに能動的にアクセスでき、 NAT デバイスは EIM テーブルエントリに基づいて宛先アドレスとポートを変換する(IP2/port2 IP1/port1 に変換)。
- NO-PAT 方式:イントラネットからアウトトラネットへのメッセージに対して、ACL permit ルールに適合していれば、アドレスグループ中のアドレスを用いて発信元アドレス変換を行い、発信元ポートを変換しない(IP 1 を IP 2 に変換).;reversible も設定されている場合は、IP 2 を介したイントラネットへの外部ネットワークからのアクティブなアクセスが許可されます。このようなメッセージには、ACL の逆マッチング(メッセージの送信元/ポートと宛先アドレス/ポートを抽出し、宛先アドレスを IP 1 に変換してから、送信元/ポートと宛先アドレス/ポートを入れ替えて ACL に一致させます。)が必要です。逆マッチング ACL のメッセージのみが変換され(宛先アドレス IP 2 を IP 1 に変換)、それ以外のメッセージは変換されません。NAT ポートブロックのダイナミックマッピングではサポートされていません。

ダイナミックアドレス変換で参照されるアドレスのグループを指定するときは、次の点に注意してください。

- アドレスグループが nat outbound 設定で参照されると、nat inbound で参照できなくなります。
- 1 つのアドレスグループが PAT 方式の nat outbound 構成で参照されると、NO-PAT 方式の nat outbound 構成では参照できなくなり、その逆もできなくなります。

- PAT 方式の nat outbound で参照されるアドレスグループにポート範囲とポートブロックパラメータが設定されていれば、一致するメッセージに対して NAT ポートブロックダイナミックマッピングが行われる。

ダイナミックアドレス変換で参照される発信 ACL を指定する場合は、次の点に注意してください。

- 1 つのインタフェースでは、ACL は 1 つの nat outbound によってのみ参照できます。
- 複数の送信方向ダイナミックアドレス変換を設定する場合、ACL を参照できない nat outbound は 1 つだけです。
- ACL 番号や名前を指定しない場合、変換対象は制限されません。
- 同じインタフェースでの送信方向ダイナミックアドレス変換設定の場合、ACL が指定された設定の優先順位は、ACL が指定されていない設定の優先順位よりも高くなります。ACL が割り当てられているダイナミックアドレス変換設定では、有効な優先順位は ACL 番号のサイズによって決まり、番号が大きいほど優先順位が高くなります。
- NAT ポートブロックのダイナミックマッピング環境では、同じインタフェースにダイナミック変換の設定を追加するときに、既存の設定の ACL ルールと一致するトラフィックがすでに存在する場合、新しい設定の ACL ルールが既存の設定の ACL ルールと重複しないようにします。

ACL を参照するアウトバウンド動的アドレス変換では、NAT ルールの一致優先順位が同じ場合、デバイスは ACL 名または ACL 番号で一致し、次のルールでは ACL 名の優先順位が ACL 番号の優先順位よりも高くなります。

- ACL 名の場合、デバイスは名前の比較結果の優先順位に従って一致します。
- ACL 番号の場合、番号が大きいほどプライオリティが高くなり、デバイスが優先的に一致します。

例

#10.110.10.0/24 ネットワークセグメントのホストメッセージをアドレス変換できるように ACL 2001 を設定します。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-ipv4-basic-2001] rule deny
[Sysname-acl-ipv4-basic-2001] quit
```

#アドレスグループ 1 を設定し、アドレスグループメンバ 202.110.10.10、202.110.10.11、202.110.10.12 を追加します。

```
[Sysname] nat address-group 1
[Sysname-address-group-1] address 202.110.10.10 202.110.10.12
[Sysname-address-group-1] quit
```

#ダイナミックアドレス変換をインタフェース GigabitEthernet1/0/1 に設定すると、アドレスグループ 1 のアドレスを使用して ACL 2001 に一致するメッセージをアドレス変換でき、変換時に TCP/UDP のポート情報が使用されます。

[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 1
[Sysname-GigabitEthernet1/0/1] quit

#インタフェース GigabitEthernet1/0/1 でアドレス変換に TCP/UDP のポート情報を使用しない場合は、次の設定を使用できます。

[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 1 no-pat
[Sysname-GigabitEthernet1/0/1] quit

#インタフェース GigabitEthernet1/0/1 インタフェースの IP アドレスを直接使用してアドレス変換を行う場合は、次の設定を使用できます。

[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001
[Sysname-GigabitEthernet1/0/1] quit

#イントラネット 10.110.10.0/24 セグメントのホストは、変換されたアドレスとしてアドレスグループ 1 のアドレスを使用して外部ネットワークにアクセスします。イントラネットのユーザがイントラネットに積極的にアクセスを開始した後、アウトトラネットのユーザが 10.110.10.0/24 ネットワークセグメントのホストに積極的にアクセスを開始し、確立されたアドレス変換テーブルエントリを使用して逆アドレス変換を行うことを許可するには、次のように構成します。

[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound 2001 address-group 1 no-pat reversible

関連コマンド

- **display nat eim**
- **display nat outbound**
- **nat mapping-behavior**

21.1.34 nat outbound port-block-group

Syntax

nat outbound port-block-group *group-id* [**rule** *rule-name*]

undo nat outbound port-block-group *group-id*

デフォルト

NAT ポートブロックのスタティックマッピング設定はありません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

group-id:ポートブロックグループの番号。範囲は 0~65535 です。

rule *rule-name*:NAT ルールの名前。1~63 文字の文字列で、大文字と小文字が区別されます。「¥」 、「/」 、「:」 、「*」 、「?」 は使用できません。」 、「<」 、「>」 、「|」 、「」、 「@」 です。このパラメータを指定しない場合、名前はありません。

説明

NAT ポートブロックのスタティックマッピングを設定するには、**nat outbound port-block-group** コマンドを使用します。

undo nat outbound port-block-group コマンドを使用して、指定した NAT ポートブロックのスタティックマッピング設定を削除します。

この設定では、インタフェースの下で指定されたポートブロックグループを参照し、ポートブロックグループ内の設定データに基づいて、固定アルゴリズムに従って各プライベート IP アドレスに静的ポートブロックを割り当て、静的ポートブロックテーブルエントリを作成します。あるプライベート IP アドレスがパブリックネットワークに接続する時、そのプライベート IP アドレスによって静的ポートブロック表項目を探し、表項目に記録されたパブリック IP アドレスを使用してアドレス変換を行い、かつ対応するポートブロックから 1 つのポートを動的に割り当てて TCP/UDP ポート変換を行う。

1 つのインタフェースで、異なるポートブロックグループに基づく複数の NAT ポートブロックスタティックマッピングを設定できます。

例

#ポートグループ 1 に基づく NAT ポートブロックスタティックマッピングをインタフェース GigabitEthernet1/0/1 のアウトバウンドで設定します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound port-block-group 1

関連コマンド

- **display nat all**
- **display nat outbound port-block-group**
- **display nat port-block**
- **nat port-block-group**

21.1.35 nat outbound rule move

Syntax

nat outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

デフォルト

送信側のダイナミック NAT ルールの位置によって一致の優先順位が決まり、上位の NAT ルールほど一致の優先順位が高くなります。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1:移動する NAT ルールの名前。

after:nat-rule-name1 を nat-rule-name2 の後ろに移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値+1 になります。

before:nat-rule-name1 を nat-rule-name2 の前に移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値は-1 になります。

nat-rule-name2:移動する NAT ルールの名前。

説明

nat outbound rule move コマンドを使用して、ダイナミック NAT ルールの出力方向の一致優先順位を調整します。

このコマンドは、NAT ルール名が指定されているダイナミック NAT に対してのみ有効です。

前に移動された NAT ルールでは、デバイスが優先的に一致します。

例

#出力方向ダイナミック NAT ルール abc を出力方向ダイナミック NAT ルール def の前に移動する。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat outbound rule move abc before def

関連コマンド

- **nat outbound**

21.1.36 nat port-block-group

Syntax

nat port-block-group *group-id*

undo nat port-block-group *group-id*

デフォルト

NAT ポートブロックグループが存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id:NAT ポートブロックグループの番号。範囲は 0~65535 です。

説明

nat port-block-group コマンドを使用して、NAT ポートブロックグループを作成し、NAT port block group view に移動します。指定された NAT ポートブロックグループがすでに存在する場合は、NAT port block group view に直接進みます。

undo nat port-block-group コマンドを使用して、指定した NAT ポートブロックグループを削除します。

作成された NAT ポートブロックグループは、NAT ポートブロックのスタティックマッピングを設定するために使用されます。ポートブロックグループには、次のものが含まれます。

- **local-ip-address** コマンドで設定された 1 つ以上のプライベートネットワークアドレスメンバ。
- **global-ip-pool** コマンドで設定された 1 つ以上のパブリックアドレスメンバ。
- **port-range** コマンドで設定されたパブリックネットワークアドレスのポート範囲。
- **block-size** コマンドで設定されたポートブロックサイズ。

NAT ポートブロックの静的マッピングを行う場合、システムは、対応するポートブロックグループの構成に基づいて、プライベート IP アドレスからパブリック IP アドレス、ポートブロックへの静的マッピング関係を計算し、静的ポートブロックテーブルエントリを作成します。

例

#1 という番号の NAT ポートブロックグループを作成します。

```
<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1]
```

関連コマンド

- **block-size**
- **display nat all**

- **display nat port-block-group**
- **global-ip-pool**
- **local-ip-address**
- **nat outbound port-block-group**
- **port-range**

21.1.37 nat server rule move

Syntax

nat server rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

デフォルト

ACL 内部サーバの NAT ルールの位置に基づいて、一致の優先順位が決定されます。一致の優先順位は、上位の NAT ルールほど高くなります。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1:移動する NAT ルールの名前。

after:nat-rule-name1 を nat-rule-name2 の後ろに移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値+1 になります。

before:nat-rule-name1 を nat-rule-name2 の前に移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値は-1 になります。

nat-rule-name2:移動する NAT ルールの名前。

説明

nat server rule move コマンドは、ACL ベースの内部サーバ NAT ルールの一致優先順位を調整するために使用されます。

このコマンドは、NAT ルール名が指定された ACL ベースの内部サーバ NAT に対してのみ有効です。

前に移動された NAT ルールでは、デバイスが優先的に一致します。

例

#ACL ベースの内部サーバ NAT ルール abc を、インタフェース GigabitEthernet1/0/1 の ACL ベースの内部サーバ NAT ルール def の前に移動します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server rule move abc before def

関連コマンド

- **nat server**

21.1.38 nat server (interface-based NAT)

Syntax

(1) 一般的な内部サーバ

- 外部ネットワークアドレスが 1 つ、外部ネットワークポートが使用されていない、または外部ネットワークポートが 1 つ

nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*] **inside** *local-address* [*local-port*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**reversible**] [**rule** *rule-name*]

undo nat server [**protocol** *pro-type*] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } [*global-port*]

- 外部ネットワークアドレスが単一、外部ネットワークポートが連続

nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2* **inside** { { *local-address* | *local-address1 local-address2* } *local-port* | *local-address local-port*1 *local-port*2 } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*]

undo nat server protocol *pro-type* **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* } *global-port1 global-port2*

- 外部ネットワークアドレスが連続している、外部ネットワークポートを使用していない、または外部ネットワークポートが 1 つしかない

nat server protocol *pro-type* **global** *global-address1 global-address2* [*global-port*] **inside** { *local-address* | *local-address1 local-address2* } [*local-port*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*]

undo nat server protocol *pro-type* **global** *global-address1 global-address2* [*global-port*]

- 外部ネットワークアドレス連続、外部ネットワークポート単一

nat server protocol *pro-type* **global** *global-address1 global-address2 global-port* **inside** *local-address local-port*1 *local-port*2 [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*]

undo nat server protocol *pro-type* **global** *global-address1 global-address2 global-port*

(2) 内部サーバのロードバランシング

nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } |

global-address1 global-address2 global-port } **inside server-group** *group-id* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] [**rule** *rule-name*]

undo nat server protocol *pro-type* **global** { { *global-address* | **current-interface** | **interface** *interface-type interface-number* } { *global-port* | *global-port1 global-port2* } | *global-address1 global-address2 global-port* }

(3) ACL ベースの内部サーバ

nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* } **inside** *local-address* [*local-port*] [**rule** *rule-name*] [**priority** *priority*]

undo nat server global { *ipv4-acl-number* | **name** *ipv4-acl-name* }

デフォルト

内部サーバが存在しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

protocol *pro-type*:プロトコルタイプを指定します。設定された内部サーバは、プロトコルタイプが TCP、UDP の場合にのみポートパラメータを指定できます。免除承諾タイプを指定しない場合、すべての免除承諾タイプのメッセージが有効になります。pro-type 次の形式で入力できます。

- 数値:1~255 の範囲で値を指定します。
- プロトコル名:icmp、tcp、udp などの値を取ります。

global:サーバがサービスを提供するエクストラネット情報を指定します。

global-address:内部サーバが外部にサービスを提供する際に外部に公開する外部ネットワークの IP アドレス。

global-address1、global-address2:エクストラネットの IP アドレスの範囲。256 を超えるアドレスは使用できません。global-address1 は開始アドレス、global-address2 は終了アドレスです。global-address2 は global-address1 より大きい必要があります。

ipv4-acl-number:ACL の番号。範囲は 2000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

current-interface:現在のインタフェースのホスト用 IP アドレスを内部サーバのエクストラネットアドレスとして使用し、 Easy IP 方式を実現する内部サーバ。

interface *interface-type interface-number*:指定したインタフェースのホスト用 IP アドレスを内部サーバのエクストラネットアドレスとして使用する、 Easy IP 方式を実現する

内部サーバを示す。interface-type interface-number は、インタフェースタイプとインタフェース番号を示します。現在サポートされているインタフェースは Loopback のみです。

global-port1, global-port2:エクストラネットのポート範囲と、内部ホストの IP アドレス範囲が一対一に対応する。global-port1 は開始ポート、global-port2 は終了ポートです。global-port2 は global-port1 より大きくなければなりません。また、ポート範囲内のポートの数は 256 より大きくできません。外部ネットワークポートは次の形式で入力できます。

- 数値:1~65535 の範囲で値を指定します。この形式は、開始ポートと終了ポートの両方でサポートされています。
- プロトコル名:http、telnet などの 1~15 文字の文字列。この形式は、開始ポートでのみサポートされています。

inside:サーバのイントラネット情報を指定する。

local-address1、local-address2:イントラネットの IP アドレス範囲の連続したセットを定義し、アウトトラネットのポート範囲と 1 対 1 で対応します。local-address1 は開始アドレス、local-address2 は終了アドレスです。local-address2 は local-address1 より大きい必要があります。アドレス範囲の数は、global-port1、global-port2 で定義されているポートの数と同じである必要があります。

local-port:内部サーバのイントラネットポート番号。次の形式で入力できます。

- 数値:1~65535 (FTP データポート番号 20 以外)の範囲で値を指定できます。
- プロトコル名:http、telnet などの 1~15 文字の文字列。

global-port:エクストラネットポート番号、デフォルト値、および値の範囲の要件は local-port の規定と一致する。

local-address:サーバのイントラネット IP アドレス。

server-group *group-id*:サーバがイントラネットに属するサーバグループ。このパラメータを指定すると、負荷分散内部サーバが構成されます。group-id は内部サーバグループの数を表し、0~65535 の範囲で値を取ります。

acl:ACL の番号または名前を指定します。このパラメータを指定すると、指定した ACL permit ルールに一致するメッセージのみが、内部サーバのマッピングテーブルを使用してアドレス変換されます。

ipv4-acl-number:ACL の番号。範囲は 2000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

reversible:プライベートネットワーク側の内部サーバが外部ネットワークに能動的にアクセスできることを示す。内部サーバが外部ネットワークにアクティブにアクセスすると、プライベートネットワークのアドレスが、内部サーバが外部にサービスを提供する外部ネットワークの IP アドレスに変換されます。

rule *rule-name*:NAT ルールの名前。1~63 文字の文字列で、大文字と小文字が区別されます。「¥」 、「/」 、「:」 、「*」 、「?」 は使用できません。」 、「<」 、「>」 、「|」 、「」、 「@」 です。このパラメータを指定しない場合、名前はありません。

priority *priority*:0~2147483647 の範囲で一致する NAT ルールの優先度。値が小さいほど優先度が高くなります。このパラメータを指定しない場合、対応する NAT ルールが最も優先されます。

説明

NAT 内部サーバを設定するには、**nat server** コマンドを使用します。これは、内部サーバの外部ネットワークアドレスとポート、および内部ネットワークアドレスとポートを定義するマッピングテーブルエントリです。

undo nat server コマンドを使用して、指定した内部サーバ構成を削除します。

この構成により、NAT 装置を利用して、内部 Web サーバ、FTP サーバ、Telnet サーバ、POP 3 サーバ、DNS サーバ等の内部ネットワークのサーバを外部ネットワークに提供することができる。これらの内部サーバは、通常のイントラネット内に配置することも、MPLS VPN インスタンス内に配置することもできます。

NAT 内部サーバは通常、NAT デバイスの Outside インタフェースに設定されます。外部ネットワークユーザは、global-address で定義された外部ネットワークアドレスと global-port で定義された外部ネットワークポートを使用して、内部ネットワークアドレスと内部ネットワークポートがそれぞれ local-address と local-port である内部サーバにアクセスできます。pro-type が TCP (プロトコル番号は 6 です)でも UDP (プロトコル番号は 17 です)でもない場合、ユーザは内部 IP アドレスと外部 IP アドレスの 1 対 1 対応しか設定できず、ポート番号間のマッピングも設定できない。

NAT 内部サーバは、内部ネットワークと外部ネットワークのアドレスとポートのマッピング関係をサポートしています。

表 21-19 NAT 内部サーバのアドレスとポートのマッピング関係

外部ネットワーク	イントラネット
エクストラネットアドレス	イントラネットアドレス
外部ネットワークアドレス、ポート番号	1つのイントラネットアドレス、1つのイントラネットポート番号
1つのエクストラネットアドレス、N個の連続するエクストラネットポート番号	• 1 つのイントラネットアドレス、1 つのイントラネットポート • N 個の連続するイントラネットアドレス、1 つのイントラネットポート番号 • 1 つのイントラネットアドレス、N 個の連続するイントラネットポート番号
N個の連続したエクストラネットアドレス	• イントラネットアドレス • N 個の連続したイントラネットアドレス

外部ネットワーク	イントラネット
N個の連続したエクストラネットアドレス連続、1つのエクストラネットポート番号	• 1 つのイントラネットアドレス、1 つのイントラネットポート番号 • N 個の連続するイントラネットアドレス、1 つのイントラネットポート番号 • 1 つのイントラネットアドレス、N 個の連続するイントラネットポート番号
1つのエクストラネットアドレス、1つのエクストラネットポート番号	内部サーバグループ
1つのエクストラネットアドレス、N個の連続するエクストラネットポート番号	
N個の連続したエクストラネットアドレス、1つのエクストラネットポート番号	
外部ネットワークアドレス(ACLによる照合)	• イントラネットアドレス • 1 つのイントラネットアドレス、1 つのイントラネットポート番号

1 つのインタフェースで設定できる nat server コマンドの数は、デバイスのモデルに依存します。同じインタフェースに設定された NAT サーバのプロトコルタイプ、エクストラネットアドレス、およびエクストラネットポート番号の組み合わせは一意である必要があり、そうでない場合は設定違反と見なされます。このルールは Easy IP 方式の NAT サーバにも適用される。各 nat server コマンドで設定できる NAT 内部サーバの数は、global-port2 と global-port1 の差、つまり NAT 内部サーバに対応するために設定されるエクストラネットポートの数です。

Easy IP 方式の NAT 内部サーバは現在のインタフェースまたは他のインタフェースの IP アドレスをそのエクストラネットアドレスとして使用するため、 Easy IP 方式の NAT 内部サーバを設定した後は、他の NAT 内部サーバがそのインタフェースの IP アドレスをそのエクストラネットアドレスとして設定しないこと、またはその逆を行うことを強く推奨する。

Easy IP 方式の NAT サーバでは、参照するインタフェースの IP アドレスが変更され、既存の他の非 Easy IP 方式の NAT サーバとの競合が発生すると、 Easy IP 方式の NAT サーバの設定が無効になる.;インタフェースアドレスが競合しない IP に変更された場合、または以前に競合していた NAT サーバが削除された場合、Easy IP モードの NAT 設定が再有効になります。

負荷均衡内部サーバを配置する時、1 つの外部ネットワークアドレスを配置し、N 個の連続する外部ネットワークポート番号は 1 つの内部サーバグループに対応し、または N 個の連続する外部ネットワークアドレスを配置し、1 つの外部ネットワークポート番号は 1

つの内部サーバグループに対応すると、内部サーバグループのメンバの個数は N より小さくてはいけなく、すなわち同一ユーザは異なる外部ネットワークアドレスまたは外部ネットワークポート番号によって同一内部ネットワークサーバの同一サービスにアクセスできない。

ACL ベースの内部サーバの場合、NAT ルールで一致するプライオリティが同じ場合、デバイスは ACL 名または ACL 番号で一致し、ACL 番号よりも優先されます。ルールは次のとおりです。

- ACL 名の場合、デバイスは名前の比較結果の優先順位に従って一致します。
- ACL 番号の場合、番号が大きいほどプライオリティが高くなり、デバイスが優先的に一致します。

例

#インタフェース GigabitEthernet1/0/1 に NAT 内部サーバを設定し、ローカルネットワーク内部の Web サーバの IP アドレスを 10.110.10.10 とし、外部から http://202.110.10.10:8080 を介して Web サーバにアクセスできるようにする。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server protocol tcp global 202.110.10.10 8080 inside 10.110.10.10 http
[Sysname-GigabitEthernet1/0/1] quit
```

#正しいサーバアドレスは 10.0.0.172 であり、ユーザ設定エラーアドレスは 192.168.0.0/24 ネットワークセグメントのアドレスであり、インタフェース GigabitEthernet1/0/1 で ACL ベースの内部サーバを設定してこのユーザ設定エラーを修正します。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 5 permit ip destination 192.168.0.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat server global 3000 inside 10.0.0.172
```

関連コマンド

- **display nat all**
- **display nat server**
- **nat server-group**

21.1.39 nat server-group

Syntax

nat server-group *group-id*

undo nat server-group *group-id*

デフォルト

内部サーバグループは存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id:サーバグループ番号。範囲は 0~65535 です。

説明

nat server-group コマンドを使用して、内部サーバグループを作成し、Internal server group view に移動します。指定した内部サーバグループがすでに存在する場合は、Internal server group view に直接移動します。

undo nat server-group コマンドは、指定された内部サーバグループを削除するために使用します。

内部サーバグループには、複数の内部サーバグループメンバ(inside ip コマンドを使用した設定)を含めることができます。

例

#1 という番号の内部サーバグループを設定します。

<Sysname> system-view
[Sysname] nat server-group 1

関連コマンド

- **display nat all**
- **display nat server-group**
- **inside ip**
- **nat server**

21.1.40 nat static enable

Syntax

nat static enable

undo nat static enable

デフォルト

NAT スタティックアドレス変換機能はオフです。

View

Interface view

定義済みユーザロール

network-admin

説明

nat static enable コマンドを使用して、インタフェースで NAT スタティックアドレス変換機能を有効にします。

undo nat static enable コマンドは、インタフェースで NAT スタティックアドレス変換機能を無効にするために使用します。

インタフェースで NAT スタティックアドレス変換が有効になると、設定されているすべてのスタティックアドレス変換マッピングがそのインタフェースで有効になります。

例

#イントラネット IP アドレス 192.168.1.1 からアウトトラネット IP アドレス 2.2.2.2 へのアウトバウンド 1 対 1 のスタティックアドレス変換を設定し、インタフェース GigabitEthernet1/0/1 でスタティックアドレス変換機能を有効にします。

<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] nat static enable

関連コマンド

- **display nat all**
- **display nat static**
- **nat static**
- **nat static net-to-net**

21.1.41 nat static inbound

Syntax

nat static inbound *global-ip local-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*]

undo nat static inbound *global-ip local-ip*

デフォルト

アドレス変換マッピングがありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

global-ip:エクストラネットの IP アドレス。

local-ip:イントラネット IP アドレス。

acl:指定されたアクセス範囲のメッセージが NAT ルールを使用してアドレス変換されることを制御する ACL の番号または名前を指定します。

ipv4-acl-number:ACL の番号。範囲は 3000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

reversible:イントラネットからアウトトラネットにアクティブにアクセスするメッセージは、この設定を使用して宛先アドレス変換を行う前に、ACL で逆方向に一致する必要があることを示します。

rule *rule-name*:NAT ルールの名前。1~63 文字の文字列で、大文字と小文字が区別されます。「¥」、「/」、「:」、「*」、「?」 は使用できません。」、「<」、「>」、「|」 、「」、 「@」 です。このパラメータを指定しない場合、名前はありません。

priority *priority*:0~2147483647 の範囲で一致する NAT ルールの優先度。値が小さいほど優先度が高くなります。このパラメータを指定しない場合、対応する NAT ルールが最も優先されます。

説明

nat static inbound コマンドは、インバウンド 1 対 1 スタティックアドレス変換マッピングを設定するために使用します。

undo nat static inbound コマンドは、指定された入力方向の 1 対 1 静的アドレス変換マッピングを削除します。

外部ネットワークから内部ネットワークへのメッセージの送信元アドレス global-ip を local-ip に変換する.;イントラネットからアウトトラネットへのメッセージに対しては、その宛先アドレス local-ip を global-ip に変換する。

参照 ACL を指定する場合は、次の点に注意してください。

- ACL が指定されていない場合、外部ネットワークから内部ネットワークへのすべてのメッセージは、この設定を使用して送信元アドレス変換を実行できます。イントラネットからアウトトラネットへのすべてのメッセージは、この設定を使用して宛先アドレス変換できます。
- ACL のみが指定され、ACL 逆マッチングが指定されていない場合(設定なし reversible)、外部ネットワークから内部ネットワークへのメッセージの送信元アドレス変換には、ACL permit ルールに一致するメッセージのみが使用されます。この設定は、イントラネットからアウトトラネットにアクティブにアクセスするメッセージの宛先アドレス変換には使用できません。

- ACL と ACL 逆マッチングの両方が指定されている場合(つまり、reversible が設定されています。)、外部ネットワークから内部ネットワークへのメッセージの送信元アドレス変換には、ACL permit ルールに一致するメッセージのみが使用されます。イントラネットからアウトトラネットにアクティブにアクセスするメッセージには、ACL 逆マッチング(メッセージの送信元アドレス/ポートと宛先アドレス/ポートを抽出し、設定に基づいて宛先アドレスを変換し、送信元アドレス/ポートと宛先アドレス/ポートを入れ替えて ACL に一致させます。)が必要です。この設定では、ACL に逆マッチングするメッセージのみが変換されます。そうでない場合は変換されません。

NAT ダイナミックアドレス変換と NAT スタティックアドレス変換の両方がインタフェースで設定されている場合は、スタティックアドレス変換が優先されます。

デバイスは、複数の入力スタティックアドレス変換マッピング(nat static inbound および nat static inbound net-to-net を含む)の設定をサポートします。

ACL を参照するインバウンド 1 対 1 スタティックアドレス変換マッピングでは、NAT ルールの一致の優先度が同じ場合、デバイスは ACL 名または ACL 番号で一致し、ACL 名の優先度は ACL 番号の優先度よりも高くなります。ルールは次のとおりです。

- ACL 名の場合、デバイスは名前の比較結果の優先順位に従って一致します。
- ACL 番号の場合、番号が大きいほどプライオリティが高くなり、デバイスが優先的に一致します。

例

#外部 IP アドレス 2.2.2.2 から内部 IP アドレス 192.168.1.1 へのインバウンドスタティックアドレス変換を設定します。

<Sysname> system-view
[Sysname] nat static inbound 2.2.2.2 192.168.1.1

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

21.1.42 nat static inbound net-to-net

Syntax

nat static inbound net-to-net *global-start-address global-end-address* **local** *local-network* { *mask-length* | *mask* } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*]

undo nat static inbound net-to-net *global-start-address global-end-address* **local** *local-network* { *mask-length* | *mask* }

デフォルト

アドレス変換マッピングがありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

global-start-address global-end-address:最大 256 個のアドレスを含むエクストラネットアドレスの範囲。global-start-address は開始アドレス、global-end-address は終了アドレスです。global-end-address は global-start-address 以上でなければなりません。同じ場合、アドレスは 1 つだけです。

local-network:イントラネットセグメントのアドレス。

mask-length:イントラネットネットワークアドレスのマスク長。範囲は 8~31 です。

mask:イントラネットアドレスのマスク。

acl:指定されたアクセス範囲のメッセージが NAT ルールを使用してアドレス変換されることを制御する ACL の番号または名前を指定します。

ipv4-acl-number:ACL の番号。範囲は 3000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

reversible:イントラネットからアウトトラネットにアクティブにアクセスするメッセージは、この設定を使用して宛先アドレス変換を行う前に、ACL で逆方向に一致する必要があることを示します。

rule *rule-name*:NAT ルールの名前。1~63 文字の文字列で、大文字と小文字が区別されます。「¥」 、「/」 、「:」 、「*」 、「?」 は使用できません。」 、「<」 、「>」 、「|」 、「」、 「@」 です。このパラメータを指定しない場合、ルールに名前がありません。

priority *priority*:0~2147483647 の範囲で一致する NAT ルールの優先度。値が小さいほど優先度が高くなります。このパラメータを指定しない場合、対応する NAT ルールは、同じクラスの NAT ルールの中で最も優先順位が低く一致します。

説明

nat static inbound net-to-net コマンドを使用して、着信側ネットワークセグメントからネットワークセグメントへのスタティックアドレス変換マッピングを設定します。

undo nat static inbound net-to-net コマンドは、指定された着信側セグメントからセグメントへのスタティックアドレス変換マッピングを削除します。

エクストラネットセグメントは開始アドレスと終了アドレスで指定され、イントラネットセグメントはイントラネットアドレスとマスクで指定されます。

エクストラネットからイントラネットへのメッセージに対しては、その発信元アドレスを用いてエクストラネットアドレスをマッチングし、発信元アドレスをイントラネットアドレスに変換する.;イントラネットからエクストラネットへのメッセージに対しては、その宛先アドレスを用いてイントラネットアドレスを照合し、宛先アドレスをエクストラネットアドレスに変換する。

エクストラネット終了アドレスは、エクストラネット開始アドレスとイントラネットマスクによって決定されるセグメント内の最大 IP アドレスより大きくすることはできません。たとえば、イントラネットアドレスを 2.2.2.0 に設定し、マスクを 255.255.255.0 に設定し、エクストラネットの開始アドレスを 1.1.1.100 に設定した場合、エクストラネットの終了アドレスは、1.1.1.0/24 セグメントで使用可能な最大 IP アドレスである 1.1.1.255 よりも大きくなることはありません。

参照 ACL を指定する場合は、次の点に注意してください。

- ACL が指定されていない場合、外部ネットワークから内部ネットワークへのすべてのメッセージは、この設定を使用して送信元アドレス変換を実行できます。イントラネットからアウトトラネットへのすべてのメッセージは、この設定を使用して宛先アドレス変換できます。
- ACL のみが指定され、ACL 逆マッチングが指定されていない場合(設定なし reversible)、外部ネットワークから内部ネットワークへのメッセージの送信元アドレス変換には、ACL permit ルールに一致するメッセージのみが使用されます。イントラネットからアウトトラネットへのメッセージでは、この設定を使用して宛先アドレス変換を行うことはできません。
- ACL と ACL 逆マッチングの両方が指定されている場合(つまり、reversible が設定されています。)、外部ネットワークから内部ネットワークへのメッセージの送信元アドレス変換には、ACL permit ルールに一致するメッセージのみが使用されます。イントラネットからアウトトラネットへのメッセージには、ACL 逆マッチング(メッセージの送信元アドレス/ポートと宛先アドレス/ポートを抽出し、設定に基づいて宛先アドレスを変換し、送信元アドレス/ポートと宛先アドレス/ポートを入れ替えて ACL に一致させます。)が必要です。この設定では、ACL 逆マッチングされたメッセージのみが変換され、それ以外は変換されません。

NAT ダイナミックアドレス変換と NAT スタティックアドレス変換の両方がインタフェースで設定されている場合は、スタティックアドレス変換が優先されます。

デバイスは複数のインバウンドスタティックアドレス変換マッピング(nat static inbound および nat static inbound net-to-net を含む)の設定をサポートします。

ACL を参照するインバウンドネットワークセグメントからネットワークセグメントへのスタティックアドレス変換マッピングでは、NAT ルールの一致優先順位が同じ場合、デバイスは ACL 名または ACL 番号で一致し、ACL 名の優先順位は ACL 番号の優先順位よりも高くなります。ルールは次のとおりです。

- ACL 名の場合、デバイスは名前の比較結果の優先順位に従って一致します。

- ACL 番号の場合、番号が大きいほどプライオリティが高くなり、デバイスが優先的に一致します。

例

#外部ネットワークセグメント 202.100.1.0/24 から内部ネットワークセグメント 192.168.1.0/24 へのインバウンドスタティックアドレス変換を設定します。

<Sysname> system-view
[Sysname] nat static inbound net-to-net 202.100.1.1 202.100.1.255 local 192.168.1.0 24

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

21.1.43 nat static inbound rule move

Syntax

nat static inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

デフォルト

入力方向 1 対 1 のスタティック NAT ルールの位置によって一致の優先順位が決まり、上位の NAT ルールほど一致の優先順位が高くなります。

View

System view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1:移動する NAT ルールの名前。

after:nat-rule-name1 を nat-rule-name2 の後ろに移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値+1 になります。

before:nat-rule-name1 を nat-rule-name2 の前に移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値は-1 になります。

nat-rule-name2:移動する NAT ルールの名前。

説明

nat static inbound rule move コマンドは、1 対 1 のインバウンドスタティック NAT ルールの一致優先順位を調整するために使用されます。

例

#着信 1 対 1 スタティック NAT ルール abc を着信 1 対 1 スタティック NAT ルール def の前に移動します。

<Sysname> system-view
[Sysname] nat static inbound rule move abc before def

関連コマンド

- **nat static inbound**

21.1.44 nat static outbound

Syntax

nat static outbound *local-ip global-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*]

undo nat static outbound *local-ip global-ip*

デフォルト

アドレス変換マッピングはありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

local-ip:イントラネット IP アドレス。

global-ip:エクストラネットの IP アドレス。

acl:指定されたアクセス範囲のメッセージが NAT ルールを使用してアドレス変換されることを制御する ACL の番号または名前を指定します。

ipv4-acl-number:ACL の番号。範囲は 3000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

reversible:この設定を使用して宛先アドレス変換を実行するには、外部ネットワークから内部ネットワークにアクティブにアクセスするメッセージが ACL で逆方向に一致する必要があることを示します。

rule *rule-name*:NAT ルールの名前。1~63 文字の文字列で、大文字と小文字が区別されます。「¥」、「/」、「:」、「*」、「?」は使用できません。」、「<」、「>」、

「|」 、「」、 「@」 です。このパラメータを指定しない場合、ルールに名前がありません。

priority *priority*:0~2147483647 の範囲で一致する NAT ルールの優先度。値が小さいほど優先度が高くなります。このパラメータを指定しない場合、対応する NAT ルールは、同じクラスの NAT ルールの中で最も優先順位が低く一致します。

説明

nat static outbound コマンドを使用して、1 対 1 のスタティックアドレス変換マッピングへの出力を設定します。

undo nat static outbound コマンドは、1 対 1 のスタティックアドレス変換マッピングを削除するために使用されます。

イントラネットからアウトトラネットへのメッセージの送信元アドレス local-ip を global-ip に変換する.;エクストラネットからイントラネットへのメッセージに対しては、その宛先アドレス global-ip を local-ip に変換する。

参照 ACL を指定する場合は、次の点に注意してください。

- ACL が指定されていない場合、イントラネットからアウトトラネットへのすべてのメッセージは、この設定を使用して送信元アドレス変換を実行できます。この設定では、外部ネットワークから内部ネットワークへのすべてのメッセージを宛先アドレスに変換できます。
- ACL のみが指定され、ACL 逆マッチングが指定されていない場合(設定なし reversible)、イントラネットからアウトトラネットへのメッセージでは、そのメッセージが ACL permit ルールに一致する場合にのみ、この設定を使用して送信元アドレス変換を実行できます。この設定は、外部ネットワークから内部ネットワークにアクティブにアクセスするメッセージの宛先アドレス変換には使用できません。
- ACL と ACL 逆マッチングの両方が指定されている場合(つまり、reversible が設定されています。)、イントラネットからアウトトラネットへのメッセージの送信元アドレス変換にこの設定を使用できるのは、メッセージが ACL permit ルールに一致する場合のみです。外部ネットワークから内部ネットワークにアクティブにアクセスするメッセージには、ACL 逆マッチング(メッセージの送信元アドレス/ポートと宛先アドレス/ポートを抽出し、設定に基づいて宛先アドレスを変換し、送信元アドレス/ポートと宛先アドレス/ポートを入れ替えて ACL に一致させます。)が必要です。この設定では、ACL に逆マッチングするメッセージのみが変換されます。そうでない場合は変換されません。

NAT ダイナミックアドレス変換と NAT スタティックアドレス変換の両方がインタフェースで設定されている場合は、スタティックアドレス変換が優先されます。

デバイスは、複数の出力スタティックアドレス変換マッピング(nat static outbound および nat static outbound net-to-net を含む)の設定をサポートします。

ACL を参照するアウトバウンド 1 対 1 のスタティックアドレス変換マッピングでは、NAT ルールの一致の優先度が同じ場合、デバイスは ACL 名または ACL 番号で一致し、ACL 名の優先度は ACL 番号の優先度よりも高くなります。ルールは次のとおりです。

- ACL 名の場合、デバイスは名前の比較結果の優先順位に従って一致します。

- ACL 番号の場合、番号が大きいほどプライオリティが高くなり、デバイスが優先的に一致します。

例

#内部 IP アドレス 192.168.1.1 から外部 IP アドレス 2.2.2.2 への発信スタティックアドレス変換マッピングを設定します。

<Sysname> system-view
[Sysname] nat static outbound 192.168.1.1 2.2.2.2

#アウトバウンドスタティックアドレス変換マッピングを設定して、イントラネットのユーザ 192.168.1.1 がアウトバウンド IP アドレス 2.2.2.2 を使用してアウトバウンドネットワークセグメント 3.3.3.0/24 時にアクセスできるようにします。

<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound 192.168.1.1 2.2.2.2 acl 3001

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

21.1.45 nat static outbound net-to-net

Syntax

nat static outbound net-to-net *local-start-address local-end-address* **global** *global-network* { *mask-length* | *mask* } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*]

undo nat static outbound net-to-net *local-start-address local-end-address* **global** *global-network* { *mask-length* | *mask* }

デフォルト

アドレス変換マッピングはありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

local-start-address local-end-address:イントラネットアドレスの範囲。アドレスの数は 256 以下にしてください。local-start-address は開始アドレス、local-end-address は終了アドレスです。local-end-address は local-start-address 以上でなければなりません。同じ場合、アドレスは 1 つだけです。

global-network:エクストラネットセグメントのアドレス。

mask-length:外部ネットワークアドレスのマスク長。範囲は 8~31 です。

mask:エクストラネットアドレスのマスク。

acl:指定されたアクセス範囲のメッセージが NAT ルールを使用してアドレス変換されることを制御する ACL の番号または名前を指定します。

ipv4-acl-number:ACL の番号。範囲は 3000~3999 です。

name *ipv4-acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

reversible:この設定を使用して宛先アドレス変換を実行するには、外部ネットワークから内部ネットワークにアクティブにアクセスするメッセージが ACL で逆方向に一致する必要があることを示します。

rule *rule-name*:NAT ルールの名前。1~63 文字の文字列で、大文字と小文字が区別されます。「¥」 、「/」 、「:」 、「*」 、「?」 は使用できません。」 、「<」 、「>」 、「|」 、「」、 「@」 です。このパラメータを指定しない場合、ルールに名前がありません。

priority *priority*:0~2147483647 の範囲で一致する NAT ルールの優先度。値が小さいほど優先度が高くなります。このパラメータを指定しない場合、対応する NAT ルールは、同じクラスの NAT ルールの中で最も優先順位が低く一致します。

説明

nat static outbound net-to-net コマンドを使用して、発信ネットワークセグメントからネットワークセグメントへのスタティックアドレス変換マッピングを設定します。

undo nat static outbound net-to-net コマンドを使用して、ネットワークセグメントからネットワークセグメントへのスタティックアドレス変換マッピングを削除します。

イントラネットセグメントは開始アドレスと終了アドレスで指定され、エクストラネットセグメントはエクストラネットアドレスとマスクで指定されます。

イントラネットからエクストラネットへのメッセージに対しては、その発信元アドレスを用いてイントラネットアドレスをマッチングし、発信元アドレスをエクストラネットアドレスに変換する.;エクストラネットからイントラネットへのメッセージに対しては、その宛先アドレスを用いてエクストラネットアドレスを照合し、宛先アドレスをイントラネットアドレスに変換する。

イントラネットの終了アドレスは、イントラネットの開始アドレスとエクストラネットマスクによって決定されるセグメント内の最大 IP アドレスより大きくすることはできま

せん。たとえば、エクストラネットアドレスを 2.2.2.0 に設定し、マスクを 255.255.255.0 に設定し、イントラネットの開始アドレスを 1.1.1.100 に設定した場合、イントラネットの終了アドレスは、1.1.1.0/24 セグメントで使用可能な最大 IP アドレスである 1.1.1.255 よりも大きくなることはありません。

参照 ACL を指定する場合は、次の点に注意してください。

- ACL が指定されていない場合、イントラネットからアウトトラネットへのすべてのメッセージは、この設定を使用して送信元アドレス変換を実行できます。この設定では、外部ネットワークから内部ネットワークへのすべてのメッセージを宛先アドレスに変換できます。
- ACL のみが指定され、ACL 逆マッチングが指定されていない場合(設定なし reversible)、イントラネットからアウトトラネットへのメッセージでは、そのメッセージが ACL permit ルールに一致する場合にのみ、この設定を使用して送信元アドレス変換を実行できます。この設定は、外部ネットワークから内部ネットワークにアクティブにアクセスするメッセージの宛先アドレス変換には使用できません。
- ACL と ACL 逆マッチングの両方が指定されている場合(つまり、reversible が設定されています。)、イントラネットからアウトトラネットへのメッセージの送信元アドレス変換にこの設定を使用できるのは、メッセージが ACL permit ルールに一致する場合のみです。外部ネットワークから内部ネットワークにアクティブにアクセスするメッセージには、ACL 逆マッチング(メッセージの送信元アドレス/ポートと宛先アドレス/ポートを抽出し、設定に基づいて宛先アドレスを変換し、送信元アドレス/ポートと宛先アドレス/ポートを入れ替えて ACL に一致させます。)が必要です。この設定では、ACL に逆マッチングするメッセージのみが変換されます。そうでない場合は変換されません。

NAT ダイナミックアドレス変換と NAT スタティックアドレス変換の両方がインタフェースで設定されている場合は、スタティックアドレス変換が優先されます。

デバイスは、複数の出力スタティックアドレス変換マッピング(nat static outbound および nat static outbound net-to-net を含む)の設定をサポートします。

ACL を参照するアウトバウンドネットワークセグメントからネットワークセグメントへのスタティックアドレス変換マッピングでは、NAT ルールの一致優先順位が同じ場合、デバイスは ACL 名または ACL 番号で一致し、ACL 名の優先順位は ACL 番号の優先順位よりも高くなります。ルールは次のとおりです。

- ACL 名の場合、デバイスは名前の比較結果の優先順位に従って一致します。
- ACL 番号の場合、番号が大きいほどプライオリティが高くなり、デバイスが優先的に一致します。

例

#内部ネットワークセグメント 192.168.1.0/24 から外部ネットワークセグメント 2.2.2.0/24 への発信スタティックアドレス変換マッピングを設定します。

<Sysname> system-view
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24

#アウトバウンドセグメントからセグメントへの静的アドレス変換マッピングを設定し、イントラネット 192.168.1.0/24 セグメントのユーザがアウトバウンドセグメント 2.2.2.0/24 のアドレスを使用して、アウトバウンドセグメント 3.3.3.0/24 時にアクセスできるようにします。

<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
[Sysname] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24 acl 3001

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

21.1.46 nat static outbound rule move

Syntax

nat static outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

デフォルト

送信方向 1 対 1 のスタティック NAT ルールの位置によって一致の優先順位が決まり、上位の NAT ルールほど一致の優先順位が高くなります。

View

System view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1:移動する NAT ルールの名前。

after:nat-rule-name1 を nat-rule-name2 の後ろに移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値+1 になります。

before:nat-rule-name1 を nat-rule-name2 の前に移動すると、nat-rule-name2 の一致優先順位の値は変更されず、nat-rule-name1 の一致優先順位の値=nat-rule-name2 の一致優先順位の値は-1 になります。

nat-rule-name2:移動する NAT ルールの名前。

説明

nat static outbound rule move コマンドを使用して、1 対 1 のスタティック NAT ルールに一致する優先順位を調整します。

このコマンドは、NAT ルール名が指定されたアウトバウンド 1 対 1 のスタティック NAT に対してのみ有効です。

前に移動された NAT ルールでは、デバイスが優先的に一致します。

例

#アウトバウンド 1 対 1 スタティック NAT ルール abc をアウトバウンド 1 対 1 NAT ルール def の前に移動します。

<Sysname> system-view
[Sysname] nat static outbound rule move abc before def

関連コマンド

- **nat static outbounde**

21.1.47 nat timestamp delete

Syntax

nat timestamp delete

undo nat timestamp delete

デフォルト

TCP SYN および SYN ACK メッセージ中のタイムスタンプを削除しない。

View

System view

定義済みユーザロール

network-admin

説明

nat timestamp delete コマンドは、TCP SYN および SYN ACK メッセージのタイムスタンプの削除を有効にします。

undo nat timestamp delete コマンドを使用して、デフォルトの状態を復元します。

PAT 方式のダイナミックアドレス変換(つまり、インタフェースに nat inbound または nat outbound コマンドが設定されている)マルチキャスト環境では、 tcp_timestams と tcp_tw_recycle の両方がサーバ上で起動されていると、 Client と Server の間で TCP コネクションが確立できない可能性がある。

上記の問題を解決するには、サーバで tcp_tw_recycle 機能をオフにするか、デバイスで TCP SYN および SYN ACK メッセージのタイムスタンプの削除機能をオンにします。

例

#TCP SYN および SYN ACK メッセージのタイムスタンプの削除を有効にします。

<Sysname> system-view
[Sysname] nat timestamp delete

関連コマンド

- **nat inbound**
- **nat outbound**

21.1.48 port-block

Syntax

port-block block-size *block-size* [**extended-block-number** *extended-block-number*]

undo port-block

デフォルト

NAT アドレスグループのポートブロックパラメータが設定されていません。

View

NAT address group view

定義済みユーザロール

network-admin

パラメータ

block-size *block-size*:ポートブロックサイズは、 1 つのポートブロックに含まれるポート数であり、 1～max_number の範囲で値をとる。ここで、max_number は 65535 です。同じ NAT アドレスグループ内では、このパラメータの値は port-range パラメータの値を超えることはできません。

extended-block-number *extended-block-number*:インクリメンタルポートブロック数。範囲は 1~5 です。割り当てられたポートブロック内のポートリソースが枯渇した場合(すべてのポートが使用される)、対応するプライベート IP アドレスがパブリックネットワークに新しい接続を開始すると、割り当てられたポートブロックからポートを取得できません。このとき、割り当てポートブロックのパブリック IP アドレスが属する NAT アドレス群にインクリメンタルポートブロック数が配置されていれば、対応するプライベート IP アドレスに対してインクリメンタルポートブロック割り当てを行うことができる。プライベート IP アドレスは、同時に最大 1+extended-block-number のポートブロックを持つことができます。

説明

ポートブロックダイナミックマッピング方式では、送信方向アドレス変換を配置する際に参照する NAT アドレスの組にポートブロックパラメータを配置する必要がある。ある

プライベート IP アドレスが初めてパブリックネットワークに接続を開始する時、マッチングする NAT アドレスグループからパブリック IP アドレスを取得し、取得したパブリック IP アドレスから動的ポートブロックを割り当て、動的ポートブロック表項目(このプライベート IP アドレスが次にパブリックへの接続を開始するときに、プライベート IP アドレスを使用してダイナミックポートブロックテーブルエントリを検索します。)を作成し、パブリック IP アドレスを使用して IP アドレス変換を行い、ポートブロックからポートを動的に割り当てて TCP/UDP ポート変換を行う。

例

#NAT アドレスグループ 2 のポートブロックパラメータを、ポートブロックサイズ 256、増分ポートブロック数 1 に設定します。

<Sysname> system-view
[Sysname] nat address-group 2
[Sysname-address-group-2] port-block block-size 256 extended-block-number 1

関連コマンド

- **nat address-group**

21.1.49 port-range

Syntax

port-range *start-port-number end-port-number*

undo port-range

デフォルト

パブリック IP アドレスのポート範囲は 1~65535 です。

View

NAT address group view

NAT port block group view

定義済みユーザロール

network-admin

パラメータ

start-port-number end-port-number:パブリック IP アドレスポートの開始ポート番号と終了ポート番号。end-port-number は start-port-number 以上である必要があります。

説明

port-range コマンドを使用してパブリック IP アドレスを設定するポート範囲。

undo port-range コマンドを使用して、デフォルトの状態を復元します。

NAT Address Group/NAT Port Block Group view でポート範囲を設定すると、NAT Address Group/NAT Port Block Group 内のパブリック IP アドレスのアドレス変換に使用できるすべてのポートが、指定したポート範囲内にある必要があります。

NAT ポートブロックグループ内でポート範囲を設定する場合は、ポート範囲をポートブロックサイズより小さくすることはできません。NAT アドレスグループ内でポート範囲を設定する場合、アドレスグループにポートブロックパラメータが設定されている場合は、ポート範囲をポートブロックサイズより小さくすることはできません。

例

#NAT アドレスグループ 1 のパブリック IP アドレスポート範囲を 1024~65535 に設定します。

<Sysname> system-view
[Sysname] nat address-group 1
[Sysname-address-group-1] port-range 1024 65535

#NAT ポートブロックグループ 1 のパブリック IP アドレスを設定するポート範囲は 30001~65535 です。

<Sysname> system-view
[Sysname] nat port-block-group 1
[Sysname-port-block-group-1] port-range 30001 65535

関連コマンド

- **nat address-group**
- **nat port-block-group**

21.1.50 reset nat session

Syntax

reset nat session [**protocol** { **tcp** | **udp** }]

View

User view

定義済みユーザロール

network-admin

パラメータ

protocol:指定したプロトコルタイプの NAT セッションを削除します。このパラメータが指定されていない場合は、すべてのプロトコルタイプの NAT セッションが削除されます。

tcp:TCP プロトコルタイプの NAT セッションを削除します。

udp:UDP プロトコルタイプの NAT セッションを削除します。

説明

NAT セッションを削除するには、**reset nat session** コマンドを使用します。

例

#NAT セッションを削除します。

<Sysname> reset nat session

関連コマンド

- **display nat session**

目次

このセクションのページは **5-x-x** です。

22 章 IP ルーティングの基本 22-1
22.1 IP ルーティングの基本設定コマンド 22-1
22.1.1 display ip routing-table 22-1
22.1.2 display ip routing-table acl 22-7
22.1.3 display ip routing-table *ip-address* 22-12
22.1.4 display ip routing-table prefix-list 22-16
22.1.5 display ip routing-table protocol 22-18
22.1.6 display ip routing-table statistics 22-19
22.1.7 reset ip routing-table statistics protocol 22-21

22章 IP ルーティングの基本

22.1 IPルーティングの基本設定コマンド

関連コマンド

- **ip load-sharing mode**

22.1.1 display ip routing-table

Syntax

display ip routing-table [**verbose**]

display ip routing-table all-routes

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all-routes:パブリックネットワークのルーティングテーブル情報を表示します。

verbose:アクティブルートと非アクティブルートを含む、すべてのルーティングテーブルの詳細を表示します。このパラメータが指定されていない場合は、アクティブなルートのサマリー情報が表示されます。

説明

display ip routing-table コマンドを使用して、ルーティングテーブルの情報を表示します。

例

#ルーティングテーブル内の現在アクティブなルートのサマリー情報を表示します。

<Sysname> display ip routing-table

Destinations：12　　Routes：12

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	Static	60	0	192.168.47.4	Vlan12

	Static 60	0	192.168.47.4	Vlan13
127.0.0.0/8	Direct 0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct 0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct 0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct 0	0	127.0.0.1	InLoop0
192.168.1.0/24	Direct 0	0	192.168.1.40	Vlan11
192.168.1.0/32	Direct 0	0	192.168.1.40	Vlan11
192.168.1.40/32	Direct 0	0	127.0.0.1	InLoop0
192.168.1.255/32	Direct 0	0	192.168.1.40	Vlan11
224.0.0.0/4	Direct 0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct 0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct 0	0	127.0.0.1	InLoop0

#パブリックネットワーク上の現在アクティブなルートのサマリー情報を表示します。

<Sysname> display ip routing-table all-routes

VPN instance: public instance

Destinations：10　　Routes：10

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct 0	0		127.0.0.1	InLoop0
1.1.1.0/24	Static 60	0		192.168.47.4	Vlan11
127.0.0.0/8	Direct 0	0		127.0.0.1	InLoop0
127.0.0.0/32	Direct 0	0		127.0.0.1	InLoop0
127.0.0.1/32	Direct 0	0		127.0.0.1	InLoop0
127.255.255.255/32	Direct 0	0		127.0.0.1	InLoop0
192.168.1.40/32	Direct 0	0		127.0.0.1	InLoop0
224.0.0.0/4	Direct 0	0		0.0.0.0	NULL0
224.0.0.0/24	Direct 0	0		0.0.0.0	NULL0
255.255.255.255/32	Direct 0	0		127.0.0.1	InLoop0

表 22-1　display ip routing-table コマンドの表示情報の説明

フィールド	説明
Destinations	宛先アドレス数
Routes	ルーティング・バー数
Destination/Mask	宛先アドレス/マスク長

フィールド	説明
Proto	そのルートのルーティングプロトコルタイプを検出します。 • Direct:直接ルーティング • Static:スタティックルート • RIP:RIP ルーティングプロトコル • OSPF:OSPF ルーティングプロトコル • O_INTRA:OSPF エリア内ルート • O_INTER:OSPF エリア間ルーティング • O_ASE 1:OSPF ファーストクラスの外部ルート • O_ASE 2:OSPF クラス 2 外部ルート • O_SUM:OSPF 集約ルート
Pre	ルートの優先順位
Cost	ルートのメトリック
NextHop	このルートのネクストホップアドレス
Interface	この宛先セグメントへのパケットは、このインタフェースから発信されます。
Summary count	ルート数

#ルーティングテーブルの詳細を表示します。

<Sysname> display ip routing-table verbose

Destinations : 13　　Routes : 13

Destination: 0.0.0.0/32
　Protocol: Direct
　Process ID: 0
　SubProtID: 0x0　　Age: 08h34m37s
　Cost: 0　　Preference: 0
　IpPre: N/A　　QosLocalID: N/A
　Tag: 0　　State: Active NoAdv
　OrigTblID: 0x0　　OrigVrf: default-vrf
　TableID: 0x2　　OrigAs: 0
　NibID: 0x10000000　　LastAs: 0
　AttrID: 0xffffffff　　Neighbor: 0.0.0.0
　Flags: 0x1000c　　OrigNextHop: 127.0.0.1
　Label: NULL　　RealNextHop: 127.0.0.1
　BkLabel: NULL　　BkNextHop: N/A
　SRLabel: NULL　　Interface: InLoopBack0
　BkSRLabel: NULL　　BkInterface: N/A

Tunnel ID: Invalid IPInterface: InLoopBack0
BkTunnel ID: Invalid BKIPInterface: N/A
InLabel: NULL ColorInterface: N/A
SIDIndex: NULL BKColorInterface: N/A
FtnIndex: 0x0 TunnelInterface: N/A
TrafficIndex: N/A BKTunnelInterface: N/A
Connector: N/A PathID: 0x0
SRTunnelID: Invalid
SID Type: N/A NID: Invalid
FlushNID: Invalid BkNID: Invalid
BkFlushNID: Invalid StatFlags: 0x0
Exp: N/A
VpnPeerId: N/A Dscp: N/A
SID: N/A OrigLinkID: 0x0
BkSID: N/A RealLinkID: 0x0
CommBlockLen: 0

Destination: 1.1.1.0/24
Protocol: Static
Process ID: 0
SubProtID: 0x0 Age: 04h20m37s
Cost: 0 Preference: 60
IpPre: N/A QosLocalID: N/A
Tag: 0 State: Active Adv
OrigTblID: 0x0 OrigVrf: default-vrf
TableID: 0x2 OrigAs: 0
NibID: 0x10000003 LastAs: 0
AttrID: 0xffffffff Neighbor: 0.0.0.0
Flags: 0x1008c OrigNextHop: 192.168.47.4
Label: NULL RealNextHop: 192.168.47.4
BkLabel: NULL BkNextHop: N/A
SRLabel: NULL Interface: Vlan-interface12
BkSRLabel: NULL BkInterface: N/A
Tunnel ID: Invalid IPInterface: Vlan-interface12
BkTunnel ID: Invalid BKIPInterface: N/A
InLabel: NULL ColorInterface: N/A
SIDIndex: NULL BKColorInterface: N/A
FtnIndex: 0x0 TunnelInterface: N/A
TrafficIndex: N/A BKTunnelInterface: N/A
Connector: N/A PathID: 0x0
SRTunnelID: Invalid
SID Type: N/A NID: Invalid
FlushNID: Invalid BkNID: Invalid

BkFlushNID: Invalid StatFlags: 0x0
Exp: N/A
VpnPeerId: N/A Dscp: N/A
SID: N/A OrigLinkID: 0x0
BkSID: N/A RealLinkID: 0x0
CommBlockLen: 0

...

表 22-2 display ip routing-table verbose コマンドの表示情報の説明

フィールド	説明
Destinations	宛先アドレス数
Routes	ルーティング・バー数
Destination	宛先アドレス/マスク
Protocol	そのルートのルーティングプロトコルタイプを検出します。 • Direct:直接ルーティング • Static:スタティックルート • RIP:RIP ルーティングプロトコル • OSPF:OSPF ルーティングプロトコル • O_INTRA:OSPF エリア内ルート • O_INTER:OSPF エリア間ルーティング • O_ASE 1:OSPF ファーストクラスの外部ルート • O_ASE 2:OSPF クラス 2 外部ルート • O_SUM:OSPF 集約ルート
Process ID	プロセス番号
SubProtID	経路制御サブプロトコルID
Age	このルートがルーティングテーブルに存在する時間
Cost	ルートのメトリック
Preference	ルートの優先順位
IpPre	IP優先度の値
QosLocalID	QoSローカルID、無効な値はN/A
Tag	ルートマーカー

フィールド	説明
State	ルーティングステータスの説明: • Active:有効なユニキャストルート • Adv:外部へのルーティングを許可 • Inactive:非アクティブなルートフラグ • NoAdv:パブリッシュされたルートは許可されていません • NAT:NAT によって生成されるルート • TunE:Tunnel トンネルの標識 • Derive:ルーティングのイテレーションの発信インタフェースが一意でない場合、最初のイテレーションルート以外のイテレーションルートをルーティングします。このタグを持つルートは、ルートエントリ数にカウントされません。
OrigTblID	元のルーティングテーブルID
OrigVrf	(未サポート)ルートが属する元のVPN。パブリックネットワークの場合はdefault-vrfと表示されます。
TableID	ルートが存在するルートテーブルのID
OrigAs	(未サポート)初期AS番号
NibID	ネクストホップID
LastAs	(未サポート)最終AS番号
AttrID	ルート属性ID番号
Neighbor	ルーティングプロトコルのネイバアドレス
Flags	経路標識ビット
OrigNextHop	このルートのネクストホップアドレス
Label	(未サポート)タブ
RealNextHop	ルーティングトゥルーネクストホップ
BkLabel	(未サポート)バックアップラベル
BkNexthop	次のホップアドレスのバックアップ
SRLabel	(未サポート) SR (Segment Routing、セグメントルーティング)タブ
BkSRLabel	(未サポート) SRバックアップラベル
SIDIndex	(未サポート) SIDのインデックス値
InLabel	(未サポート)ルーティングタグ
Tunnel ID	トンネルID
Interface	この宛先セグメントへのパケットは、このインタフェースから発信されます。
BkTunnel ID	バックアップトンネルID
BkInterface	インタフェースのバックアップ
IPInterface	IP発信インタフェース
BkIPInterface	バックアップIPアウトインタフェース
ColorInterface	(未サポート) Color出力、つまりSR-MPLS TE Policy反復による出力
BkColorInterface	(未サポート)バックアップColorインタフェース外

フィールド	説明
FtnIndex	FTNテーブルエントリインデックス
TunnelInterface	Tunnelインタフェースを出力
TrafficIndex	トラフィック統計インデックス値。範囲は1~64で、N/Aは無効です。
BkTunnelInterface	バックアップTunnelインタフェース
Connector	(未サポート)は、BGPがMD VPNプロパティを保持するConnector属性を示します。これは、VPN-IPv4ルートを交換するときにピアが送信元PEのアドレスを保持することを意味します。N/Aは、この属性がないことを示します。
Summary count	ルート数
PathID	パスID
SRTunnelID	(未サポート) SRトンネルID
SID Type	(未サポート) SIDタイプ。N/Aは属性がありません。
NID	ルーティングプロトコルでブラッシングされたNHLFE (Next Hop Label Forwarding Entry、次のホップラベル転送エントリ)テーブルエントリのインデックス
FlushNID	実際にFIBにフラッシュされたNHLFEテーブルエントリのインデックス
BkNID	ルーティングプロトコルでブラッシュアップされたバックアップNHLFEテーブルエントリインデックス
BkFlushNID	実際にFIBにフラッシュされたバックアップNHLFEテーブルエントリのインデックス
StatFlags	(未サポート) SRv 6トラフィック統計タグ
VpnPeerId	(未サポート)ルートが属するVPN peer IDの値は1~134217727の範囲で、N/Aは無効です。
Dscp	0~63の範囲でルーティングされたDSCP優先順位、無効な値はN/A
Exp	ルートのEXP優先度(BGPサポートのみ)、N/Aは無効な値
SID	(未サポート)主にSID (Segment Identifier、セグメントID)を使用します。N/Aは属性がないことを示します。
BkSID	(未サポート)代替SID、N/Aは属性なし
CommBlockLen	(未サポート) Locatorの共通プレフィックス長
OrigLinkID	SDWAN TTE接続元のLink ID
RealLinkID	SDWAN TTE実際の接続Link ID

22.1.2 display ip routing-table acl

Syntax

display ip routing-table acl *ipv4-acl-number* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv4-acl-number:ベース ACL の番号。範囲は 2000~2999 です。

verbose:指定した ACL でフィルタリングされたすべてのルートの詳細を表示します。このパラメータが指定されていない場合、指定された ACL によってフィルタリングされたアクティブなルートのサマリー情報のみが表示されます。

説明

display ip routing-table acl コマンドは、指定された ACL によってフィルタリングされたルーティング情報を表示するために使用します。

ユーザが指定した ACL が存在しない場合、または ACL にルールがない場合は、すべてのルーティング情報が表示されます。

例

#ACL 2000 を設定し、ルートフィルタルールを設定します。

<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any

#ACL 2000 でフィルタリングされたアクティブルートのサマリー情報を表示します。

[Sysname-acl-ipv4-basic-2000] display ip routing-table acl 2000

Summary count：4

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
192.168.1.0/24	Direct	0	0	192.168.1.111	Vlan11
192.168.1.0/32	Direct	0	0	192.168.1.111	Vlan11
192.168.1.111/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.255/32	Direct	0	0	192.168.1.111	Vlan11

上記の説明については、表 22-1 を参照してください。

#ACL 2000 でフィルタリングされたすべてのルートの詳細を表示します。

<Sysname> display ip routing-table acl 2000 verbose

Summary count：4

Destination: 192.168.1.0/24
Protocol: Direct

```
Process ID: 0
SubProtID: 0x1                    Age: 04h20m37s
Cost: 0                       Preference: 0
IpPre: N/A                    QosLocalID: N/A
Tag: 0                            State: Active Adv
OrigTblID: 0x0                OrigVrf: default-vrf
TableID: 0x2                      OrigAs: 0
NibID: 0x10000003                 LastAs: 0
AttrID: 0xffffffff            Neighbor: 0.0.0.0
Flags: 0x10080                OrigNextHop: 192.168.1.111
Label: NULL                   RealNextHop: 192.168.1.111
BkLabel: NULL                     BkNextHop: N/A
SRLabel: NULL                     Interface: Vlan-interface11
BkSRLabel: NULL               BkInterface: N/A
Tunnel ID: Invalid            IPInterface: Vlan-interface11
BkTunnel ID: Invalid          BKIPInterface: N/A
InLabel: NULL                 ColorInterface: N/A
SIDIndex: NULL                BKColorInterface: N/A
FtnIndex: 0x0                 TunnelInterface: N/A
TrafficIndex: N/A             BKTunnelInterface: N/A
Connector: N/A                    PathID: 0x0
SRTunnelID: Invalid
SID Type: N/A                     NID: Invalid
FlushNID: Invalid                 BkNID: Invalid
BkFlushNID: Invalid           StatFlags: 0x0
Exp: N/A
VpnPeerId: N/A                    Dscp: N/A
SID: N/A                  OrigLinkID: 0x0
BkSID: N/A                RealLinkID: 0x0
CommBlockLen: 0

Destination: 192.168.1.0/32
Protocol: Direct
Process ID: 0
SubProtID: 0x0                    Age: 04h20m37s
Cost: 0                       Preference: 0
IpPre: N/A                    QosLocalID: N/A
Tag: 0                            State: Active NoAdv
OrigTblID: 0x0                OrigVrf: default-vrf
TableID: 0x2                      OrigAs: 0
NibID: 0x10000003                 LastAs: 0
AttrID: 0xffffffff            Neighbor: 0.0.0.0
Flags: 0x1008c                OrigNextHop: 192.168.1.111
```

```
        Label: NULL                RealNextHop: 192.168.1.111
      BkLabel: NULL                  BkNextHop: N/A
      SRLabel: NULL                  Interface: Vlan-interface11
    BkSRLabel: NULL                BkInterface: N/A
    Tunnel ID: Invalid               IPInterface: Vlan-interface11
  BkTunnel ID: Invalid             BKIPInterface: N/A
     InLabel: NULL                ColorInterface: N/A
     SIDIndex: NULL              BKColorInterface: N/A
     FtnIndex: 0x0               TunnelInterface: N/A
 TrafficIndex: N/A             BKTunnelInterface: N/A
    Connector: N/A                    PathID: 0x0
  SRTunnelID: Invalid
     SID Type: N/A                      NID: Invalid
     FlushNID: Invalid                BkNID: Invalid
   BkFlushNID: Invalid              StatFlags: 0x0
          Exp: N/A
   VpnPeerId: N/A                     Dscp: N/A
          SID: N/A               OrigLinkID: 0x0
        BkSID: N/A               RealLinkID: 0x0
 CommBlockLen: 0

 Destination: 192.168.1.111/32
    Protocol: Direct
  Process ID: 0
    SubProtID: 0x1                    Age: 04h20m37s
        Cost: 0                  Preference: 0
       IpPre: N/A                QosLocalID: N/A
         Tag: 0                      State: Active NoAdv
    OrigTblID: 0x0                OrigVrf: default-vrf
     TableID: 0x2                  OrigAs: 0
       NibID: 0x10000000            LastAs: 0
      AttrID: 0xffffffff          Neighbor: 0.0.0.0
       Flags: 0x10004             OrigNextHop: 127.0.0.1
       Label: NULL                RealNextHop: 127.0.0.1
     BkLabel: NULL                  BkNextHop: N/A
     SRLabel: NULL                  Interface: InLoopBack0
   BkSRLabel: NULL                BkInterface: N/A
   Tunnel ID: Invalid               IPInterface: InLoopBack0
 BkTunnel ID: Invalid             BKIPInterface: N/A
    InLabel: NULL                ColorInterface: N/A
    SIDIndex: NULL              BKColorInterface: N/A
    FtnIndex: 0x0               TunnelInterface: N/A
TrafficIndex: N/A             BKTunnelInterface: N/A
```

Connector: N/A PathID: 0x0
SRTunnelID: Invalid
SID Type: N/A NID: Invalid
FlushNID: Invalid BkNID: Invalid
BkFlushNID: Invalid StatFlags: 0x0
Exp: N/A
VpnPeerId: N/A Dscp: N/A
SID: N/A OrigLinkID: 0x0
BkSID: N/A RealLinkID: 0x0
CommBlockLen: 0

Destination: 192.168.1.255/32
Protocol: Direct
Process ID: 0
SubProtID: 0x0 Age: 04h20m37s
Cost: 0 Preference: 0
IpPre: N/A QosLocalID: N/A
Tag: 0 State: Active NoAdv
OrigTblID: 0x0 OrigVrf: default-vrf
TableID: 0x2 OrigAs: 0
NibID: 0x10000003 LastAs: 0
AttrID: 0xffffffff Neighbor: 0.0.0.0
Flags: 0x1008c OrigNextHop: 192.168.1.111
Label: NULL RealNextHop: 192.168.1.111
BkLabel: NULL BkNextHop: N/A
SRLabel: NULL Interface: Vlan-interface11
BkSRLabel: NULL BkInterface: N/A
Tunnel ID: Invalid IPInterface: Vlan-interface11
BkTunnel ID: Invalid BKIPInterface: N/A
InLabel: NULL ColorInterface: N/A
SIDIndex: NULL BKColorInterface: N/A
FtnIndex: 0x0 TunnelInterface: N/A
TrafficIndex: N/A BKTunnelInterface: N/A
Connector: N/A PathID: 0x0
SRTunnelID: Invalid
SID Type: N/A NID: Invalid
FlushNID: Invalid BkNID: Invalid
BkFlushNID: Invalid StatFlags: 0x0
Exp: N/A
VpnPeerId: N/A Dscp: N/A
SID: N/A OrigLinkID: 0x0
BkSID: N/A RealLinkID: 0x0
CommBlockLen: 0

. . .

上記の説明は、表 22-2 を参照してください。

22.1.3 display ip routing-table *ip-address*

Syntax

display ip routing-table *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *ip-address1* **to** *ip-address2* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address:宛先 IP アドレス 0 は 10 進数形式です。

mask-length:ネットマスクの長さ。範囲は 0~32 です。

mask:ネットマスク 0 の 10 進数形式。

longer-match:指定された宛先ネットワークに一致するすべてのルーティング情報を表示します。一致条件の詳細については、下記の説明に記載します。

ip-address1 **to** *ip-address2*:IP アドレス範囲。ip-address1 と ip-address2 は一緒にアドレス範囲を決定し、その範囲内のアドレスを持つルートのみが表示されます。

verbose:アクティブルートと非アクティブルートを含む、すべてのルーティングテーブルの詳細を表示します。このパラメータが指定されていない場合は、アクティブなルートのサマリー情報が表示されます。

説明

display ip routing-table ip-address コマンドは、指定された宛先アドレスのルーティング情報を表示します。

display ip routing-table ip-address1 to ip-address2 コマンドは、指定された宛先アドレス範囲のルーティング情報を表示します。

コマンドの出力は、さまざまなオプションパラメータを使用して異なります。次に、コマンドの出力例を示します。

(1) display ip routing-table ip-address

次の条件を満たすすべてのアクティブルートを表示します。

- ユーザが入力した宛先 IP アドレスは、ルーティングテーブル中の各ルートのサブネットマスク値と演算されます.;

- ルーティングテーブル内の各ルートの宛先 IP アドレスは、自身のサブネットマスク値と演算されます。
- 結果が同じルートエントリが表示されます。

(2) display ip routing-table ip-address mask

次の条件を満たすすべてのアクティブルートを表示します。

- ユーザが入力した宛先 IP アドレスは、ユーザが入力したサブネットマスク値と比較されます。
- ルーティングテーブル中の各ルートの宛先 IP アドレスはユーザが入力したサブネットマスク値と演算する.;
- 結果は同じで、ユーザが入力したサブネットマスク以下のマスクを持つルートエントリが表示されます。

(3) display ip routing-table ip-address longer-match

次の条件を満たすすべてのアクティブルートを表示します。

- ユーザが入力した宛先 IP アドレスは、次の 3 つの場合にサブネットマスク値と一致します。
  - ユーザが入力した宛先 IP アドレスはそれに対応する自然ネットワーク段を得て、この自然ネットワーク段に対応するサブネットマスクデフォルト値(クラス A、B、C の IP アドレスに対するサブネットマスクのデフォルト値は、それぞれ 255.0.0.0、255.255.0.0、255.255.255.0 です。)を取り、そしてユーザが入力した宛先 IP アドレスと対応するサブネットマスクデフォルト値を演算する。
  - ユーザが宛先 IP アドレスとして 0.0.0.0 を入力すると、マスク 0.0.0.0 が使用されます。
  - 上記 2 つの場合(ループバックアドレス)を除き、マスク 255.255.255.255 を使用して、ユーザが入力した宛先 IP アドレスと AND 演算されます。
- ルーティングテーブル内の各ルートの宛先 IP アドレスは、前の手順で取得したサブネットマスク値と一致します。
- 結果が同じであるすべてのルートエントリが表示されます。

(4) display ip routing-table ip-address mask longer-match

次の条件を満たすすべてのアクティブルートを表示します。

- ユーザが入力した宛先 IP アドレスは、ユーザが入力したサブネットマスク値と比較されます。
- ルーティングテーブル中の各ルートの宛先 IP アドレスはユーザが入力したサブネットマスク値と演算する.;
- 結果が同じであるすべてのルートエントリが表示されます。

(5) display ip routing-table ip-address1 to ip-address2

宛先アドレスとマスク(32 ビット)の両方が指定された範囲内にある ip-address1/32 から ip-address2/32 までのアクティブなルートを表示します。

例

#宛先アドレスが 11.0.0.1 のルーティング情報を表示します。

<Sysname> display ip routing-table 11.0.0.1

Summary count : 3

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.0.0.0/8	Static	60	0	0.0.0.0	NULL0
11.0.0.0/16	Static	60	0	0.0.0.0	NULL0
11.0.0.0/24	Static	60	0	0.0.0.0	NULL0

#宛先アドレス/マスクが 11.0.0.1/20 のルーティング情報を表示します。

<Sysname> display ip routing-table 11.0.0.1 20

Summary count : 2

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.0.0.0/8	Static	60	0	0.0.0.0	NULL0
11.0.0.0/16	Static	60	0	0.0.0.0	NULL0

#宛先アドレスが 11.0.0.1 で、一致条件を満たすルーティング情報を表示します。

<Sysname> display ip routing-table 11.0.0.1 longer-match

Summary count : 3

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.0.0.0/8	Static	60	0	0.0.0.0	NULL0
11.0.0.0/16	Static	60	0	0.0.0.0	NULL0
11.0.0.0/24	Static	60	0	0.0.0.0	NULL0

#宛先アドレス/マスクが 11.0.0.1/20 で、一致条件を満たすルーティング情報を表示します。

<Sysname> display ip routing-table 11.0.0.1 20 longer-match

Summary count : 3

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.0.0.0/8	Static	60	0	0.0.0.0	NULL0
11.0.0.0/16	Static	60	0	0.0.0.0	NULL0
11.0.0.0/24	Static	60	0	0.0.0.0	NULL0

#宛先アドレス 1.1.1.0~5.5.5.0 の範囲のルーティング情報を表示します。

<Sysname> display ip routing-table 1.1.1.0 to 5.5.5.0

Summary count : 4

```
Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.1.1.1/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0           2.2.2.1         Vlan2
3.3.3.1/32          Direct 0    0           127.0.0.1       InLoop0
4.4.4.1/32          Direct 0    0           127.0.0.1       InLoop0
```

#宛先アドレスが 1.2.3.4 のルートの詳細を表示します。

```
<Sysname> display ip routing-table 1.2.3.4 verbose

Summary count : 1

Destination: 1.2.3.4/32
   Protocol: Static
  Process ID: 0
   SubProtID: 0x1                    Age: 00h00m37s
       Cost: 0                Preference: 60
      IpPre: N/A              QosLocalID: N/A
        Tag: 0                    State: Active Adv
   OrigTblID: 0x0                OrigVrf: default-vrf
     TableID: 0x2                OrigAs: 0
       NibID: 0x15000000           LastAs: 0
      AttrID: 0x0               Neighbor: 0.0.0.0
       Flags: 0x10060          OrigNextHop: 192.168.47.2
       Label: NULL            RealNextHop: 192.168.47.2
     BkLabel: NULL              BkNextHop: N/A
     SRLabel: NULL              Interface: Vlan-interface11
   BkSRLabel: NULL             BkInterface: N/A
   Tunnel ID: Invalid           IPInterface: Vlan-interface11
 BkTunnel ID: Invalid         BKIPInterface: N/A
     InLabel: NULL           ColorInterface: N/A
    SIDIndex: NULL         BKColorInterface: N/A
    FtnIndex: 0x0           TunnelInterface: N/A
TrafficIndex: N/A         BKTunnelInterface: N/A
   Connector: N/A                  PathID: 0x0
  SRTunnelID: Invalid
    SID Type: N/A                    NID: Invalid
    FlushNID: Invalid               BkNID: Invalid
  BkFlushNID: Invalid             StatFlags: 0x0
         Exp: N/A
   VpnPeerId: N/A                    Dscp: N/A
         SID: N/A          OrigLinkID: 0x0
       BkSID: N/A          RealLinkID: 0x0
CommBlockLen: 0
```

上記の説明は、表 22-1 を参照してください。

22.1.4 display ip routing-table prefix-list

Syntax

display ip routing-table prefix-list *prefix-list-name* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

prefix-list-name:接頭辞リスト名。1~63 文字の文字列で、大文字と小文字が区別されます。

verbose:このパラメータを使用すると、フィルタルールを通過するすべてのルートの詳細が表示されます。このパラメータが指定されていない場合、フィルタルールを通過するアクティブなルートのサマリー情報のみが表示されます。

説明

display ip routing-table prefix-list コマンドは、指定したプレフィックスリストでフィルタリングされたルート情報を表示します。

指定したプレフィックスリストが存在しない場合は、すべてのルーティング情報が表示されます。

例

#アドレスプレフィックスリストの設定 test プレフィックス 1.1.1.0、マスク長 24 のルートを許可します。

<Sysname> system-view
[Sysname] ip prefix-list test permit 1.1.1.0 24

#プレフィックスリスト test でフィルタリングされたアクティブルートのサマリー情報を表示します。

[Sysname] display ip routing-table prefix-list test

Summary count：1

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.1.1.0/24	Direct	0	0	1.1.1.2	Vlan11

上記の説明は、表 22-1 を参照してください。

#プレフィックスリスト test でフィルタリングされたすべてのルートの詳細を表示します。

[Sysname] display ip routing-table prefix-list test verbose

```
Summary count : 1

Destination: 1.1.1.0/24
    Protocol: Direct
  Process ID: 0
   SubProtID: 0x1                    Age: 04h20m37s
        Cost: 0                  Preference: 0
       IpPre: N/A                QosLocalID: N/A
         Tag: 0                     State: Active Adv
   OrigTblID: 0x0                 OrigVrf: default-vrf
     TableID: 0x2                  OrigAs: 0
       NibID: 0x10000003           LastAs: 0
      AttrID: 0xffffffff         Neighbor: 0.0.0.0
       Flags: 0x1008c            OrigNextHop: 1.1.1.2
       Label: NULL               RealNextHop: 1.1.1.2
     BkLabel: NULL                 BkNextHop: N/A
     SRLabel: NULL                 Interface: Vlan-interface11
   BkSRLabel: NULL               BkInterface: N/A
   Tunnel ID: Invalid            IPInterface: Vlan-interface11
BkTunnel ID: Invalid           BKIPInterface: N/A
     InLabel: NULL             ColorInterface: N/A
     SIDIndex: NULL          BKColorInterface: N/A
     FtnIndex: 0x0           TunnelInterface: N/A
TrafficIndex: N/A          BKTunnelInterface: N/A
   Connector: N/A                  PathID: 0x0
  SRTunnelID: Invalid
    SID Type: N/A                    NID: Invalid
    FlushNID: Invalid                BkNID: Invalid
  BkFlushNID: Invalid              StatFlags: 0x0
         Exp: N/A
   VpnPeerId: N/A                    Dscp: N/A
         SID: N/A              OrigLinkID: 0x0
       BkSID: N/A              RealLinkID: 0x0
CommBlockLen: 0
```

上記の説明は、表 22-2 を参照してください。

22.1.5 display ip routing-table protocol

Syntax

display ip routing-table protocol *protocol* [**inactive** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

protocol:指定されたルーティングプロトコルに関する情報を表示します。

inactive:非アクティブなルートに関する情報を表示します。このパラメータが指定されていない場合は、アクティブルートと非アクティブルートの情報が表示されます。

verbose:このパラメータを使用すると、ルートの詳細が表示されます。このパラメータが指定されていない場合は、ルートのサマリー情報が表示されます。

説明

display ip routing-table protocol コマンドは、指定されたプロトコルによって生成または検出されたルート情報を表示するために使用します。

例

#すべての直接ルートのサマリー情報を表示します。

<Sysname> display ip routing-table protocol direct

Summary count : 9

Direct Routing table status : <Active>
Summary count : 9

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
2.2.2.0/24	Direct	0	0	2.2.2.1	Vlan2
2.2.2.0/32	Direct	0	0	2.2.2.1	Vlan2
2.2.2.2/32	Direct	0	0	127.0.0.1	InLoop0
2.2.2.255/32	Direct	0	0	2.2.2.1	Vlan2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

Direct Routing table status：<Inactive>
Summary count：0

#静的ルーティングテーブルを表示します。

<Sysname> display ip routing-table protocol static

Summary count：1

Static Routing table status：<Active>
Summary count：0

Static Routing table status：<Inactive>
Summary count：1

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.2.3.0/24	Static	60	0	1.2.4.5	Vlan10

22.1.6 display ip routing-table statistics

Syntax

display ip routing-table [**all-routes**] [**prefix**] **statistics**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all-routes:パブリックネットワークの情報を表示します。

prefix:プレフィックスの統計情報を表示します。このパラメータを指定しない場合、ルートの統計情報が表示されます。

説明

display ip routing-table statistics コマンドを使用して、ルーティングテーブル内のルートまたはプレフィックスの統計情報を表示します。

パラメータを指定しない場合は、パブリックネットワークの情報が表示されます。

例

#ルーティングテーブルの包括的なルーティング統計情報を表示します。

<Sysname> display ip routing-table statistics

Total prefixes: 15　　Active prefixes: 15

Proto	Routes	Active	Added	Deleted
DIRECT	12	12	30	18
STATIC	3	3	5	2
UNR	0	0	0	0
RIP	0	0	0	0
OSPF	0	0	0	0
IS-IS	0	0	0	0
LISP	0	0	0	0
EIGRP	0	0	0	0
BGP	0	0	0	0
OpenR	0	0	0	0
Total	15	15	35	20

#パブリックネットワークのプレフィックス統計を表示します。

<Sysname> display ip routing-table prefix statistics

Proto	Prefixes	Active	Added	Deleted
DIRECT	7	7	7	0
STATIC	0	0	0	0
UNR	0	0	0	0
RIP	1	0	1	0
OSPF	0	0	0	0
IS-IS	0	0	0	0
LISP	0	0	0	0
EIGRP	0	0	0	0
BGP	0	0	0	0
OpenR	0	0	0	0
Total	8	7	8	0

表 22-3　display ip routing-table statistics コマンドの表示情報の説明

フィールド	説明
Total prefixes	接頭辞の合計数
Active prefixes	アクティブなプレフィックスの合計数
Proto	ルーティングプロトコル、直接ルーティングと静的ルーティングのみをサポート
Route	総ルート数
Prefixes	プレフィックス数
Active	アクティブな使用中のルートの数

フィールド	説明
Added	ルータが起動した後、またはルーティングテーブルが最後にクリアされた後に、ルーティングテーブルに追加されたルートの数
Deleted	削除対象としてマークされたルートの数(このようなルートは、しばらく待つと解放されます。)
Total	さまざまなタイプのルート数の合計

22.1.7 reset ip routing-table statistics protocol

Syntax

reset ip routing-table statistics protocol { *protocol* | **all** }

reset ip routing-table [**all-routes**] **statistics protocol** { *protocol* | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all-routes:パブリックネットワークのルーティング統計をクリアします。

protocol:IPv 4 ルーティングテーブルで指定されたルーティングプロトコルの統計情報をクリアします。

all:IPv 4 ルーティングテーブル内のすべてのルーティングプロトコルの統計情報をクリアします。

説明

reset ip routing-table statistics protocol コマンドは、ルーティングテーブルからルーティング統計情報をクリアするために使用します。

all-routes パラメータが指定されていない場合は、パブリックネットワークのルーティング統計がクリアされます。

例

#ルーティングテーブルからルーティング統計情報をクリアします。

<Sysname> reset ip routing-table statistics protocol all

目次

このセクションのページは **5-x-x** です。

23 章 スタティックルーティング 23-1
23.1 スタティックルーティング設定コマンド 23-1
23.1.1 delete static-routes all 23-1
23.1.2 ip route-static 23-2
23.1.3 ip route-static default-preference 23-4

23章 スタティックルーティング

23.1 スタティックルーティング設定コマンド

23.1.1 delete static-routes all

Syntax

delete static-routes all

View

System view

定義済みユーザロール

network-admin

説明

delete static-routes all コマンドを使用して、すべてのスタティックルートを削除します。

 注意

すべてのスタティックルートを削除すると、ネットワークが不通になり、メッセージ転送が失敗する場合があります。この場合は注意して使用してください。

このコマンドを使用してスタティックルートを削除すると、設定されているすべてのスタティックルートが削除されるまで、確認メッセージが表示されます。

スタティックルートを削除するには **undo ip route-static** コマンドを使用し、デフォルトルートを含むすべてのスタティックルートを削除するには **delete static-routes all** コマンドを使用します。

例

#すべてのスタティックルートを削除します。

<Sysname> system-view

[Sysname] delete static-routes all

```
This will erase all IPv4 static routes and their configurations, you must reconf
igure all static routes.
Are you sure?[Y/N]:y
```

関連コマンド

- **ip route-static**

23.1.2 ip route-static

Syntax

ip route-static *dest-address* { *mask-length* | *mask* } { *interface-type interface-number* [*next-hop-address*] [**backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*] [**permanent**] | **permanent** | *next-hop-address* [**permanent**] | **permanent** } [**preference** *preference*] [**recursive-lookup**] [**description** *text*]

ip route-static *dest-address* { *mask-length* | *mask* } *next-hop-address* [**nexthop-index** *index-string*] [**permanent**] [**preference** *preference*] [**recursive-lookup**] [**description** *text*]

ip route-static group *group-name interface-type interface-number* [*next-hop-address*] [**backup-interface** *interface-type interface-number* [**backup-nexthop** *backup-nexthop-address*] [**permanent**] | **permanent**] [**preference** *preference*] [**recursive-lookup**] [**description** *text*]

ip route-static group *group-name next-hop-address* [**permanent**] [**preference** *preference*] [**recursive-lookup**] [**description** *text*]

undo ip route-static { *dest-address* { *mask-length* | *mask* } | **group** *group-name* } [*interface-type interface-number* [*next-hop-address*] | *next-hop-address*]

デフォルト

スタティックルートが設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

dest-address:スタティックルートの宛先 IP アドレス 0 の 10 進数形式。

mask-length:ネットマスクの長さ。範囲は 0~32 です。

mask:ネットマスク 0 の 10 進数形式。

group *group-name*:スタティックルート設定グループを指定します。group-name は、構成グループ名を示す 1~31 文字の文字列で、大文字と小文字が区別されます。

interface-type interface-number:スタティックルートの出力インタフェースタイプとインタフェース番号を指定します。

next-hop-address:ルートのネクストホップの IP アドレスを 10 進数 0 で指定します。

nexthop-index *index-string*:ルートのネクストホップのインデックス ID を指定します。index-string はインデックス ID を示す 1~93 文字の文字列で、大文字と小文字は区別されません。このパラメータが指定されていない場合、スタティックルートは、発信インタフェースとネクストホップの IP アドレスをインデックス ID として使用します。同じ宛先に向かう複数のルートのネクストホップのインデックス ID は同じではありません。

backup-interface *interface-type interface-number*:インタフェースをバックアップします。バックアップアウトインタフェースが非 P 2 P タイプのインタフェース(NBMA タイプインタフェースまたはブロードキャストタイプインタフェースを含む)の場合は、対応するバックアップネクストホップアドレスも指定する必要があります。interface-type interface-number は、指定されたインタフェースのタイプと番号です。

backup-nexthop *backup-nexthop-address*:ネクストホップアドレスをバックアップします。

permanent:永続的な静的ルートとして指定します。設定された永続的なスタティックルートは、インタフェースがダウンしても active のままです。

preference *preference*:スタティックルートの優先度を 1~255 の範囲で指定します。デフォルト値は 60 です。

recursive-lookup:スタティックルートのネクストホップ反復(つまり、より大きなセグメントへの反復ルーティングが可能になります。)機能を有効にします。このパラメータを指定しない場合、スタティックルートのネクストホップ反復処理がオフになります。

description *text*:1~60 文字の範囲で設定されたスタティックルート記述情報。「?」 以外に、スペースなどの特殊文字を含めることができます。

各パラメータの設定についての注意事項は、以下の説明に記載します。

説明

スタティックルートを設定するには、**ip route-static** コマンドを使用します。

undo ip route-static コマンドを使用して、指定したスタティックルートを削除します。

宛先 IP アドレスとマスクが両方とも 0.0.0.0 (マスクが 0 の場合)の場合、構成されたルートがデフォルトルートになります。一致するルーティングテーブルエントリがない場合、メッセージ転送にはデフォルトルートが使用されます。

異なる優先順位設定では、異なるルーティング管理ポリシーを使用できます。たとえば、同じ宛先に対して複数のルートを構成し、同じ優先度を指定すると、ルートの負荷分散が可能になります。異なる優先度を指定すると、ルートバックアップが実装されます。

スタティックルートを設定する場合、必要に応じてインタフェースまたはネクストホップアドレスを指定できます。次の点に注意してください。

- Null0 インタフェースの場合、発信インタフェースが設定されていれば、ネクストホップアドレスを設定する必要はありません。
- ポイントツーポイントインタフェースの場合は、インタフェースだけを指定し、ネクストホップアドレスを指定しないで設定できます。これにより、ピアアドレスが変更されても構成を変更する必要がなくなります。

- NBMA, P 2 MP などのインタフェースでは、IP アドレスからリンク層アドレスへのマッピングが必要であり、インタフェースとネクストホップ IP アドレスの両方を配置することを推奨する。
- ブロードキャストタイプのインタフェースでは、複数のネクストホップが存在する可能性があるため、インタフェースとネクストホップ IP アドレスの両方を設定する必要があります。

設定グループごとにスタティックルートを設定すると、設定グループのすべてのプレフィックスに同じネクストホップ、アウトインタフェース情報が適用されます。

スタティックルートのルートイテレーションでは、反復ルートの宛先アドレス範囲にスタティックルートの宛先アドレスが含まれている場合、たとえば、スタティックルート 10.1.0.0/24 の反復ルートの宛先アドレスが 10.1.0.0/16 の場合、反復が発生したとみなされます。スタティックルートのネクストホップループイテレーションが有効になる前に、ループイテレーションによってこのイテレーションが失敗し、ルートイテレーションが続行されます。スタティックルートのネクストホップループイテレーションを有効にすると、反復ルートの出力インタフェースがデバイスの直接接続された出力インタフェースである限り、反復ループが発生しても、この反復は成功と見なされます。ループイテレーションによって検出されたインタフェースのスタティックルートは、他のルーティングプロトコルによって他のデバイスにパブリッシュできません。

パラメータ recursive-lookup host-route と recursive-lookup は相互に排他的であり、同時に設定することはできません。

例

#宛先アドレスが 1.1.1.1/24 で、ネクストホップが 2.2.2.2、説明情報が「for internet」であるスタティックルートを設定します。

<Sysname> system-view

[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 description for internet

関連コマンド

- **display ip routing-table protocol (ネットワーク接続/IP ルーティングの基本)**
- **ip route-static-group**
- **prefix**

23.1.3 ip route-static default-preference

Syntax

ip route-static default-preference *default-preference*

undo ip route-static default-preference

デフォルト

スタティックルートのデフォルトの優先順位は 60 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

default-preference:スタティックルートのデフォルトの優先度の値。範囲は 1~255 です。

説明

スタティックルートのデフォルトの優先順位を設定するには、**ip route-static default-preference** コマンドを使用します。

undo ip route-static default-preference コマンドを使用して、デフォルトの状態を復元します。

スタティックルートを設定するときに優先順位を指定しない場合、デフォルトの優先順位が使用されます。

デフォルトの優先度を再構成すると、新しく設定されたデフォルトの優先度は、新しく追加された静的ルートに対してのみ有効になります。

例

#スタティックルートの設定のデフォルトの優先順位は 120 です。

<Sysname> system-view

[Sysname] ip route-static default-preference 120

関連コマンド

- **display ip routing-table protocol (ネットワーク接続/IP ルーティングの基本)**

目次

このセクションのページは **5-x-x** です。

24 章 IGMP スヌーピング 24-1
24.1 IGMP スヌーピング設定コマンド 24-1
24.1.1 display igmp-snooping 24-1
24.1.2 display igmp-snooping group 24-4
24.1.3 display igmp-snooping router-port 24-6
24.1.4 display igmp-snooping static-group 24-7
24.1.5 display igmp-snooping static-router-port 24-9
24.1.6 display igmp-snooping statistics 24-10
24.1.7 display l2-multicast ip forwarding 24-11
24.1.8 display l2-multicast mac forwarding 24-12
24.1.9 dot1p-priority (IGMP-Snooping view) 24-13
24.1.10 dscp 24-14
24.1.11 entry-limit (IGMP-Snooping view) 24-15
24.1.12 fast-leave (IGMP-Snooping view) 24-16
24.1.13 group-policy (IGMP-Snooping view) 24-17
24.1.14 host-aging-time (IGMP-Snooping view) 24-18
24.1.15 igmp-snooping 24-19
24.1.16 igmp-snooping dot1p-priority 24-20
24.1.17 igmp-snooping drop-unknown 24-21
24.1.18 igmp-snooping { disable | enable } 24-22
24.1.19 igmp-snooping fast-leave 24-23
24.1.20 igmp-snooping general-query source-ip 24-25
24.1.21 igmp-snooping group-limit 24-26
24.1.22 igmp-snooping group-policy 24-27
24.1.23 igmp-snooping host-aging-time 24-28
24.1.24 igmp-snooping host-join 24-29
24.1.25 igmp-snooping last-member-query-interval 24-31
24.1.26 igmp-snooping leave source-ip 24-32
24.1.27 igmp-snooping max-response-time 24-33
24.1.28 igmp-snooping overflow-replace 24-34
24.1.29 igmp-snooping querier 24-35
24.1.30 igmp-snooping query-interval 24-36
24.1.31 igmp-snooping report source-ip 24-37
24.1.32 igmp-snooping router-aging-time 24-38
24.1.33 igmp-snooping special-query source-ip 24-40
24.1.34 igmp-snooping static-group 24-41

24.1.35 igmp-snooping static-router-port 24-42
24.1.36 igmp-snooping version 24-43
24.1.37 last-member-query-interval (IGMP-Snooping view) 24-44
24.1.38 max-response-time (IGMP-Snooping view) 24-45
24.1.39 overflow-replace (IGMP-Snooping view) 24-46
24.1.40 report-aggregation (IGMP-Snooping view) 24-47
24.1.41 reset igmp-snooping group 24-47
24.1.42 reset igmp-snooping router-port 24-48
24.1.43 reset igmp-snooping statistics 24-49
24.1.44 router-aging-time (IGMP-Snooping view) 24-49

24章 IGMP スヌーピング

24.1 IGMPスヌーピング設定コマンド

24.1.1 display igmp-snooping

Syntax

display igmp-snooping [**global** | **vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global:IGMP Snooping のグローバルステータス情報を表示します。

vlan *vlan-id*:指定した VLAN 内の IGMP Snooping のステータス情報を表示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。

説明

display igmp-snooping コマンドは、IGMP Snooping のステータス情報を表示するために使用します。

オプションのパラメータを指定しない場合は、グローバルおよびすべての VLAN で IGMP Snooping のステータス情報が表示されます。

例

#グローバルおよびすべての VLAN の IGMP Snooping ステータス情報を表示します。

<Sysname> display igmp-snooping
IGMP snooping information: Global
 Global-enable: Enabled
 Drop-unknown: Disabled
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Report-aggregation: Enabled
 Host-tracking: Disabled

```
 Dot1p-priority: --

IGMP snooping information: VLAN 1
 IGMP snooping: Enabled
 Drop-unknown: Disabled
 Version: 2
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: 2
 Proxy: Disabled

IGMP snooping information: VLAN 10
 IGMP snooping: Enabled
 Drop-unknown: Enabled
 Version: 3
 Host-aging-time: 260s
 Router-aging-time: 260s
 Max-response-time: 10s
 Last-member-query-interval: 1s
 Querier: Enabled (IP: 1.1.1.1, Expires: 00:02:05)
 Querier-election: Enabled
 Query-interval: 125s
 General-query source IP: 1.1.1.1
 Special-query source IP: 2.2.2.2
 Report source IP: 3.0.0.3
 Leave source IP: 1.0.0.1
 Host-tracking: Disabled
 Dot1p-priority: --
 Proxy: Disabled
```

表 24-1　display igmp-snooping コマンドの表示情報の説明

フィールド	説明
IGMP snooping information	IGMP Snoopingのステータス情報

フィールド	説明
Global-enable	IGMP Snoopingのグローバルイネーブル状態: • Enabled:グローバルが有効であることを示す • Disabled:グローバルが無効であることを示します。
IGMP snooping	IGMP Snooping単一VLAN内のイネーブル状態: • Enabled:が有効であることを示します。 • Disabled:無効であることを示します。 • Globally enabled:グローバル機能を表します。 • Inactive:IGMP Snooping 設定が有効ではありません
Drop-unknown	不明なマルチキャストパケットをドロップする機能がオンになっています。 • Enabled:オンになっていることを示します。 • Disabled:オンになっていないことを示します。 • Globally enabled:グローバルにオンになっていることを示します。
Version	バージョンIGMP Snooping
Host-aging-time	動的メンバポートのエージングタイム
Router-aging-time	ダイナミックルータポートのエージング時間
Max-response-time	IGMP汎用グループクエリの最大応答時間
Last-member-query-interval	IGMP特定グループ照会メッセージの送信間隔
Report-aggregation	IGMPメンバシップは、メッセージ抑制機能がオンになっていることを報告します。 • Enabled:オンになっていることを示します。 • Disabled:オンになっていないことを示します。
Dot1p-priority	IGMPメッセージの802.1 pプライオリティ「--」は、設定されていないことを示します。
Querier	IGMP Snoopingクエリアが開いている状態: • Enabled:オンになっていることを示します。 • Disabled:オンになっていないことを示します。
(IP:1.1.1.1, Expires:00:02:05)	IGMP Snoopingクエラー情報: • IP:クエラーの IP アドレスを表します。 • Expires:クエリアのエージングタイムの残り時間を示します。 IGMP Snoopingクエリが開いていない場合、上記のフィールドは表示されません。

フィールド	説明
Querier-election	IGMP Snoopingクエラー選挙機能オン状態: • Enabled:オンになっていることを示します。 • Disabled:オンになっていないことを示します。
Query-interval	IGMP汎用グループクエリメッセージの送信間隔
General-query source IP	IGMP汎用グループクエリメッセージの送信元IPアドレス
Special-query source IP	IGMP特定グループクエリメッセージの送信元IPアドレス
Report source IP	IGMPメンバシップレポートメッセージの送信元IPアドレス
Leave source IP	IGMPがグループメッセージの送信元IPアドレスから離れる
Host-tracking	IGMP Snoopingホスト追跡機能がオンになっている • Enabled:オンになっていることを示します。 • Disabled:オンになっていないことを示します。 • Globally enabled:グローバルにオンになっていることを示します。
Proxy	IGMP Snooping Proxy開いた状態: • Enabled:オンになっていることを示します。 • Disabled:オンになっていないことを示します。

24.1.2 display igmp-snooping group

Syntax

display igmp-snooping group [*group-address* | *source-address*] * [**vlan** *vlan-id*][**interface** *interface-type interface-number* | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-address:指定されたマルチキャストグループの情報を 224.0.1.0~239.255.255.255 の範囲で表示します。このパラメータを指定しない場合は、すべてのマルチキャストグループの情報が表示されます。

source-address:指定されたマルチキャストソースの情報を表示します。このパラメータを指定しない場合、すべてのマルチキャストソースの情報が表示されます。

vlan *vlan-id*:指定した VLAN 内の情報を表示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。このパラメータを指定しないと、すべての VLAN の情報が表示されます。

interface *interface-type interface-number*:指定されたインタフェースが属するダイナミック IGMP Snooping マルチキャストグループに関する簡単な情報を表示します。このパラメータが指定されていない場合は、すべてのインタフェースに関する情報が表示されます。

verbose:詳細を表示します。このパラメータが指定されていない場合は、簡単な情報が表示されます。

説明

display igmp-snooping group コマンドは、ダイナミック IGMP Snooping マルチキャストグループの情報を表示するために使用されます。

例

#インタフェース GigabitEthernet1/0/1 が属するダイナミック IGMP Snooping マルチキャストグループの情報を表示します。

```
<Sysname> display igmp-snooping group interface gigabitethernet 1/0/1
Total 1 entries.

GE1/0/1:
  VLAN 2: Total 1 entries.
   (0.0.0.0, 224.1.1.1)                    (00:03:23)
```

#VLAN 2 内のダイナミック IGMP Snooping マルチキャストグループの詳細を表示します。

```
<Sysname> display igmp-snooping group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2                               (00:03:23)
          Outer VLAN 5       Inner VLAN 2             (00:03:35)
```

表 24-2　display igmp-snooping group コマンドの表示情報の説明

フィールド	説明
Total 1 entries	テーブルアイテムの合計数
VLAN 2:Total 1 entries	VLAN 2内のテーブルエントリの合計数
(0.0.0.0、224.1.1.1)	(S, G)テーブルエントリ。0.0.0.0はすべてのマルチキャストソースを表します。

フィールド	説明
Attribute	次のようなテーブルアイテムのプロパティ • global port:テーブルエントリにグローバルポートが存在することを示します。 • local port:このデバイスのポートがテーブルエントリに存在することを示します。
FSM information	次のようなテーブルアイテムステートマシン • delete:すべてのメンバ属性が削除されたことを示します。 • dummy:新しく作成された一時テーブルエントリを表します。 • no info:テーブルエントリが存在しないことを示します。
Host slots (0 in total)	このフィールドは実用的ではありません
Host ports (1 in total)	メンバポートおよび合計数
(00:03:23)	メンバポートのエージングタイムの残り時間

関連コマンド

- **reset igmp-snooping group**

24.1.3 display igmp-snooping router-port

Syntax

display igmp-snooping router-port [**vlan** *vlan-id*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose:詳細を表示します。このパラメータが指定されていない場合は、簡単な情報が表示されます。

vlan *vlan-id*:指定した VLAN 内の情報を表示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。このパラメータを指定しないと、すべての VLAN の情報が表示されます。

説明

display igmp-snooping router-port コマンドを使用して、ダイナミックルータポートの情報を表示します。

例

#VLAN 2 内のダイナミックルータポートに関する簡単な情報を表示します。

```
<Sysname> display igmp-snooping router-port vlan 2
VLAN 2:
  Router ports (2 in total):
    GE1/0/1                  (00:01:30)
    GE1/0/2                  (00:00:23)
```

#VLAN 2 のダイナミックルータポートの詳細を表示します。

```
<Sysname> display igmp-snooping router-port vlan 2 verbose
VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1                  (00:01:30)
    GE1/0/2                  (00:00:23)
```

表 24-3　display igmp-snooping router-port コマンドの表示情報の説明

フィールド	説明
VLAN 2	VLANの番号
Router slots (0 in total)	このフィールドは実用的ではありません
Router ports (2 in total)	ダイナミックルータポートと合計数
(00:01:30)	ダイナミックルータポートのエージングタイムの残り時間

関連コマンド

- **reset igmp-snooping router-port**

24.1.4 display igmp-snooping static-group

Syntax

display igmp-snooping static-group [*group-address* | *source-address*] * [**vlan** *vlan-id*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-address:指定されたマルチキャストグループの情報を 224.0.1.0~239.255.255.255 の範囲で表示します。このパラメータを指定しない場合は、すべてのマルチキャストグループの情報が表示されます。

source-address:指定されたマルチキャストソースの情報を表示します。このパラメータを指定しない場合、すべてのマルチキャストソースの情報が表示されます。

vlan *vlan-id*:指定した VLAN 内の情報を表示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。このパラメータを指定しないと、すべての VLAN の情報が表示されます。

verbose:詳細を表示します。このパラメータが指定されていない場合は、簡単な情報が表示されます。

説明

display igmp-snooping static-group コマンドは、スタティック IGMP Snooping マルチキャストグループの情報を表示するために使用されます。

例

#VLAN 2 内のスタティック IGMP Snooping マルチキャストグループの詳細を表示します。

```
<Sysname> display igmp-snooping static-group vlan 2 verbose
Total 1 entries.

VLAN 2: Total 1 entries.
  (0.0.0.0, 224.1.1.1)
    Attribute: local port
    FSM information: dummy
    Host slots (0 in total):
    Host ports (1 in total):
      GE1/0/2
```

表 24-4　display igmp-snooping static-group コマンドの表示情報の説明

フィールド	説明
Total 1 entries	テーブルアイテムの合計数
VLAN 2:Total 1 entries	VLAN 2内のテーブルエントリの合計数
(0.0.0.0、224.1.1.1)	(S, G)テーブルエントリ。0.0.0.0はすべてのマルチキャストソースを表します。
Attribute	次のようなテーブルアイテムのプロパティ ● global port:テーブルエントリにグローバルポートが存在することを示します。 ● local port:このデバイスのポートがテーブルエントリに存在することを示します。

フィールド	説明
FSM information	次のようなテーブルアイテムステートマシン • delete:すべてのメンバ属性が削除されたことを示します。 • dummy:新しく作成された一時テーブルエントリを表します。 • no info:テーブルエントリが存在しないことを示します。
Host slots (0 in total)	このフィールドは実用的ではありません
Host ports (1 in total)	メンバポートおよび合計数

24.1.5 display igmp-snooping static-router-port

Syntax

display igmp-snooping static-router-port [**vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*:指定した VLAN 内の情報を表示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。

verbose:詳細を表示します。このパラメータが指定されていない場合は、簡単な情報が表示されます。

説明

display igmp-snooping static-router-port コマンドを使用して、スタティックルータポートの情報を表示します。

例

#VLAN 2 内のスタティックルータポートに関する簡単な情報を表示します。

<Sysname> display igmp-snooping static-router-port vlan 2

VLAN 2:

Router ports (2 in total):

GE1/0/1

GE1/0/2

#VLAN 2 内のスタティックルータポートの詳細を表示します。

<Sysname> display igmp-snooping static-router-port vlan 2 verbose

VLAN 2:
  Router slots (0 in total):
  Router ports (2 in total):
    GE1/0/1
    GE1/0/2

表 24-5　display igmp-snooping static-router-port コマンドの表示情報の説明

フィールド	説明
VLAN 2	VLANの番号
Router slots (0 in total)	このフィールドは実用的ではありません
Router ports (2 in total)	静的ルータポートと合計数

24.1.6 display igmp-snooping statistics

Syntax

display igmp-snooping statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display igmp-snooping statistics コマンドは、IGMP Snooping が受信する IGMP メッセージの統計情報を表示するために使用されます。

例

#IGMP Snooping が受信した IGMP メッセージの統計情報を表示します。

<Sysname> display igmp-snooping statistics
Received IGMP general queries: 0
Received IGMPv1 reports: 0
Received IGMPv2 reports: 19
Received IGMP leaves: 0
Received IGMPv2 specific queries: 0
Sent IGMPv2 specific queries: 0
Received IGMPv3 reports: 1
Received IGMPv3 reports with right and wrong records: 0
Received IGMPv3 specific queries: 0
Received IGMPv3 specific sg queries: 0

Sent　IGMPv3 specific queries:　0

Sent　IGMPv3 specific sg queries:　0

Received PIMv2 hello:　0

Received error IGMP messages:　19

表 24-6　display igmp-snooping statistics コマンドの表示情報の説明

フィールド	説明
general queries	IGMP汎用グループクエリメッセージの数
specific queries	IGMP固有のグループクエリメッセージの数
reports	IGMPメンバシップ・レポートのメッセージ数
leaves	IGMP離脱グループメッセージの数
reports with right and wrong records	エラーと正しいレコードを含むIGMPメンバシップレポートメッセージの数
specific sg queries	IGMP特定のソースグループのクエリメッセージの数
PIMv2 hello	(未サポート) PIMv2 helloメッセージ数
error IGMP messages	エラーIGMPメッセージの数

関連コマンド

- **reset igmp-snooping statistics**

24.1.7 display l2-multicast ip forwarding

Syntax

display l2-multicast ip forwarding [**group** *group-address* | **source** *source-address*]*[**vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group *group-address*:指定されたマルチキャストグループの情報を表示します。このパラメータを指定しない場合は、すべてのマルチキャストグループの情報が表示されます。

source *source-address*:指定されたマルチキャストソースの情報を表示します。このパラメータを指定しない場合、すべてのマルチキャストソースの情報が表示されます。

vlan *vlan-id*:指定した VLAN 内の情報を表示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。このパラメータを指定しないと、すべての VLAN の情報が表示されます。

説明

display l2-multicast ip forwarding コマンドは、レイヤ 2 マルチキャストの IP 転送テーブル情報を表示するために使用されます。

例

#VLAN 2 内のレイヤ 2 マルチキャストの IP 転送テーブル情報を表示します。

<Sysname> display l2-multicast ip forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
(0.0.0.0, 224.1.1.1)
Host ports (3 in total):
GigabitEthernet1/0/1
GigabitEthernet1/0/2
GigabitEthernet1/0/3

表 24-7　display l2-multicast ip forwarding コマンドの表示情報の説明

フィールド	説明
Total 1 entries	テーブルアイテムの合計数
VLAN 2:Total 1 entries	VLAN 2内のテーブルエントリの合計数
(0.0.0.0、224.1.1.1)	(S, G)テーブルエントリ。0.0.0.0はすべてのマルチキャストソースを表します。
Host ports (3 in total)	メンバポートおよび合計数

24.1.8 display l2-multicast mac forwarding

Syntax

display l2-multicast mac forwarding [*mac-address*] [**vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address:指定された MAC マルチキャストグループの情報を表示します。このパラメータを指定しないと、すべての MAC マルチキャストグループの情報が表示されます。

vlan *vlan-id*:指定した VLAN 内の情報を表示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。このパラメータを指定しないと、すべての VLAN の情報が表示されます。

説明

display l2-multicast mac forwarding コマンドは、レイヤ 2 マルチキャストの MAC 転送テーブル情報を表示するために使用されます。

例

#VLAN 2 内のレイヤ 2 マルチキャストの MAC 転送テーブル情報を表示します。

```
<Sysname> display l2-multicast mac forwarding vlan 2
Total 1 entries.

VLAN 2: Total 1 entries.
  MAC group address: 0100-5e01-0101
    Host ports (3 in total):
      GigabitEthernet1/0/1
      GigabitEthernet1/0/2
      GigabitEthernet1/0/3
```

表 24-8　display l2-multicast mac forwarding コマンドの表示情報の説明

フィールド	説明
Total 1 entries	テーブルアイテムの合計数
VLAN 2:Total 1 entries	VLAN 2内のテーブルエントリの合計数
MAC group address	MACマルチキャストグループのアドレス
Host ports (3 in total)	メンバポートおよび合計数

24.1.9 dot1p-priority (IGMP-Snooping view)

Syntax

dot1p-priority *priority*

undo dot1p-priority

デフォルト

IGMP メッセージの 802.1 p プライオリティが設定されていません。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

priority:0~7 の範囲の IGMP メッセージの 802.1 p 優先順位。この値が大きいほど、優先順位が高くなります。

説明

IGMP メッセージの 802.1 p プライオリティをグローバルに設定するには、**dot1p-priority** コマンドを使用します。

undo dot1p-priority コマンドを使用して、デフォルトの状態を復元します。

VLAN ベースの設定の場合、このコマンドの機能は **igmp-snooping dot1p-priority** コマンドと同じですが、範囲が異なります。IGMP-snooping view でのグローバル設定はすべての VLAN で有効で、VLAN view での設定は現在の VLAN でのみ有効で、VLAN view での設定は優先順位が高くなります。

例

#IGMP メッセージの 802.1 p 優先順位を 3 にグローバルに設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dot1p-priority 3

関連コマンド

- **igmp-snooping dot1p-priority**

24.1.10 dscp

Syntax

dscp *dscp-value*

undo dscp

デフォルト

デバイスが IGMP プロトコルメッセージを送信する DSCP の優先順位は 48 です。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

dscp-value:DSCP 値。範囲は 0~63 です。

説明

dscp コマンドを使用して、デバイスが IGMP プロトコルメッセージを送信する DSCP プライオリティを設定します。

undo dscp コマンドを使用して、デフォルトの状態を復元します。

DSCP (Differentiated Services Code Point、Differentiated Services Encoding Point)は IP メッセージ中の ToS フィールドを持ち、メッセージ自体の優先順位を表し、メッセージ転送の優先度を決定する。DSCP 優先度の値が大きいほど、メッセージの優先度は高くなります。

例

#IGMP プロトコルメッセージを送信するデバイスの DSCP プライオリティを 63 に設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] dscp 63

24.1.11 entry-limit (IGMP-Snooping view)

Syntax

entry-limit *limit*

undo entry-limit

デフォルト

IGMP Snooping 転送テーブルエントリのグローバルな最大数は 4294967295 です。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

limit:IGMP Snooping が転送するテーブルエントリの最大グローバル数を 0~4294967295 の範囲で指定します。

説明

entry-limit コマンドは、IGMP Snooping 転送エントリ(動的テーブルエントリと静的テーブルエントリを含む)のグローバルな最大数を設定するために使用します。

undo entry-limit コマンドを使用して、デフォルトの状態を復元します。

例

#設定 IGMP Snooping 転送テーブルエントリのグローバルな最大数は 512 です。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] entry-limit 512

24.1.12 fast-leave (IGMP-Snooping view)

Syntax

fast-leave [**vlan** *vlan-list*]

undo fast-leave [**vlan** *vlan-list*]

デフォルト

fast-leave 機能がオフになっています。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*:指定された VLAN が設定されていることを示します。vlan-list は、1 つまたは複数の VLAN を表す VLAN リストで、vlan-list ={vlan-id [to vlan-id]}&<1-10>のように表示されます。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、すべての VLAN が設定されます。

説明

fast-leave コマンドは、ポートの fast-leave 機能をグローバルにオンにするために使用します。

undo fast-leave コマンドは、ポートの fast-leave 機能をグローバルにオフするために使用されます。

本機能を使用すると、デバイスはポートが leave メッセージを受信したときに、マルチキャストグループの転送エントリからポートをすぐに削除できます。

Interface view でポートの fast-leave 機能を有効にすることも、IGMP-snooping view ですべてのポートに対してグローバルに有効にすることもできます。ポートの場合、ポート設定がグローバル設定よりも優先されます。

例

#VLAN 2 内のポートファーストアウト機能をグローバルにオンにします。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] fast-leave vlan 2

関連コマンド

- **igmp-snooping fast-leave**

24.1.13 group-policy (IGMP-Snooping view)

Syntax

group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo group-policy [**vlan** *vlan-list*]

デフォルト

マルチキャストグループフィルタが設定されていません。つまり、ホストは任意の正当なマルチキャストグループに参加できます。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number:IPv 4 基本 ACL または拡張 ACL の番号を 2000~3999 の範囲で指定します。ホストは、ACL ルールで許可されているマルチキャストグループにのみ参加できます。指定された ACL が存在しない場合、または ACL に有効なルールが設定されていない場合は、すべてのマルチキャストグループが除外されます。

vlan *vlan-list*:指定された VLAN が設定されていることを示します。vlan-list は、1 つまたは複数の VLAN を表す VLAN リストで、vlan-list ={vlan-id [to vlan-id]}&<1-10>のように表示されます。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、すべての VLAN が設定されます。

説明

group-policy コマンドは、ホストが参加できるマルチキャストグループを制限するために、マルチキャストグループフィルタをグローバルに設定するために使用されます。

undo group-policy コマンドは、マルチキャストグループフィルタをグローバルに削除するために使用します。

このコマンドは、ダイナミックマルチキャストグループに対してのみ有効で、スタティックマルチキャストグループに対しては無効です。

このコマンドは、**igmp-snooping group-policy** コマンドと同じですが、スコープが異なります。IGMP-snooping view の下のグローバル設定はすべてのポートに対して有効であり、Interface view の下の設定は現在のポートに対してのみ有効であり、後者の設定は優先度が高くなります。

IPv 4 の指定 ACL を使用する場合は、次の点に注意してください。

- IPv 4 ベース ACL の場合、ACL ルールの source パラメータは、IGMP メッセージのマルチキャストグループアドレスの範囲を指定するために使用され、source、fragment、time-range 以外のオプションのパラメータは無視されます。
- IPv 4 拡張 ACL の場合、ACL ルールの source パラメータは IGMP メッセージのマルチキャスト送信元アドレス(IGMPv1/v2 メッセージと、マルチキャスト送信元アドレスを持たない IS_EX/TO_EX タイプの IGMPv3 メッセージの場合、マルチキャスト送信元アドレスが 0.0.0.0 であるとします。)の範囲を指定し、destination パラメータはマルチキャストグループアドレスの範囲を指定します。source、destination、fragment、time-range 以外のオプションのパラメータは無視されます。
- ポートごとに異なる ACL ルールを異なる VLAN に設定できますが、同じ VLAN に設定された新しいルールが古いルールに置き換わります。

例

#マルチキャストグループフィルタをグローバルに設定して、VLAN 2 内のホストがマルチキャストグループ 225.1.1.1 にのみ参加できるようにします。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

関連コマンド

- **igmp-snooping group-policy**

24.1.14 host-aging-time (IGMP-Snooping view)

Syntax

host-aging-time *seconds*

undo host-aging-time

デフォルト

ダイナミックメンバポートのエージングタイムは 260 秒です。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds:ダイナミックメンバポートのエージングタイムを秒単位で 1~8097894 の範囲で指定します。

説明

host-aging-time コマンドを使用して、ダイナミックメンバポートのエージングタイムをグローバルに設定します。

undo host-aging-time コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、**igmp-snooping host-aging-time** コマンドと同じですが、範囲が異なります。IGMP-snooping view の下のグローバル設定はすべての VLAN で有効で、VLAN view の下の設定は現在の VLAN でのみ有効で、後者の設定は優先順位が高くなります。

マルチキャストグループメンバの誤った削除を避けるため、ダイナミックメンバポートのエージングタイムが、IGMP ユニバーサルグループクエリメッセージの送信間隔と IGMP ユニバーサルグループクエリの最大応答時間の合計よりも大きくなるように設定してください。ダイナミックメンバポートのエージングタイムは、IGMP ユニバーサルグループクエリメッセージの送信間隔と IGMP ユニバーサルグループクエリの最大応答時間の合計の 2 倍に設定することをお勧めします。

例

#グローバル設定ダイナミックメンバポートのエージングタイムは 300 秒です。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] host-aging-time 300

関連コマンド

- **igmp-snooping host-aging-time**

24.1.15 igmp-snooping

Syntax

igmp-snooping

undo igmp-snooping

デフォルト

デバイスの IGMP Snooping プロパティがオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

igmp-snooping コマンドを使用して、デバイスの IGMP Snooping プロパティをオンにし、IGMP-snooping view に移動します。

undo igmp-snooping コマンドは、デバイスの IGMP Snooping プロパティをオフにします。

デバイスの IGMP Snooping 機能をオフにすると、すべての VLAN の IGMP Snooping がオフになります。

例

#デバイスの IGMP Snooping プロパティをオンにして、IGMP-snooping view に移動します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping]

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**
- **igmp-snooping disable**

24.1.16 igmp-snooping dot1p-priority

Syntax

igmp-snooping dot1p-priority *priority*

undo igmp-snooping dot1p-priority

デフォルト

IGMP メッセージの 802.1 p プライオリティが設定されていません。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

priority:0~7 の範囲の IGMP メッセージの 802.1 p 優先順位。この値が大きいほど、優先順位が高くなります。

説明

VLAN 内で IGMP メッセージの 802.1 p プライオリティを設定するには、**igmp-snooping dot1p-priority** コマンドを使用します。

undo igmp-snooping dot1p-priority コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

VLAN ベースの設定の場合、このコマンドの機能は dot1p-priority コマンドと同じですが、範囲が異なります。IGMP-snooping view でのグローバル設定はすべての VLAN で有効で、VLAN view での設定は現在の VLAN でのみ有効で、VLAN view での設定は優先順位が高くなります。

例

#VLAN 2 で IGMP Snooping を有効にし、IGMP メッセージの 802.1 p 優先順位を 3 に設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping dot1p-priority 3

関連コマンド

- **dot1p-priority (IGMP-Snooping view)**
- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**

24.1.17 igmp-snooping drop-unknown

Syntax

igmp-snooping drop-unknown

undo igmp-snooping drop-unknown

デフォルト

不明なマルチキャストデータメッセージを破棄する機能は、不明なマルチキャストデータメッセージをブロードキャストするためにオフになっています。

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping drop-unknown コマンドを使用して、VLAN 内で不明なマルチキャストデータグラムのドロップを有効にします。

undo igmp-snooping drop-unknown コマンドを使用して、VLAN 内の不明なマルチキャストデータグラムのドロップ機能をオフにします。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

このコマンドは、drop-unknown コマンドと同じですが、範囲が異なります。IGMP-snooping view の下のグローバル設定はすべての VLAN で有効で、VLAN view の下の設定は現在の VLAN でのみ有効で、後者の設定は優先順位が高くなります。

このコマンドと drop-unknown コマンドの設定は相互排他的です。つまり、IGMP-snooping view で不明なマルチキャストデータメッセージをドロップする機能がグローバルに有効になっている場合、VLAN view でこの機能を有効または無効にすることはできません。

例

#VLAN 2 で IGMP Snooping を有効にし、不明なマルチキャストデータグラムのドロップを有効にします。

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping drop-unknown
```

関連コマンド

- **drop-unknown (IGMP-Snooping view)**
- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**

24.1.18 igmp-snooping { disable | enable }

Syntax

igmp-snooping { **disable** | **enable** }

undo igmp-snooping

デフォルト

VLAN 内の IGMP Snooping の状態は、グローバルな IGMP Snooping の状態と同じです。

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping enable コマンドは単一 VLAN 内の IGMP Snooping を可能にするのに使用されます。

igmp-snooping disable コマンドは、単一の VLAN 内で IGMP Snooping をシャットダウンするために使用されます。

undo igmp-snooping コマンドは、単一の VLAN 内で IGMP Snooping の状態を現在のグローバル IGMP Snooping の状態に戻すために使用されます。

単一 VLAN 内で IGMP Snooping を使用できるようにするには、System view で igmp-snooping を設定する必要があります。

VLAN ベースの設定の場合、このコマンドの機能は enable コマンドと同じですが、範囲が異なります。IGMP-snooping view では指定された VLAN を設定でき、VLAN view では現在の VLAN のみを設定できます。設定の優先順位は同じです。

例

#デバイスの IGMP Snooping 機能をオンにし、VLAN 2 で IGMP Snooping を有効にします。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable

#VLAN 2 で IGMP Snooping を閉じます。

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping disable

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping**

24.1.19 igmp-snooping fast-leave

Syntax

igmp-snooping fast-leave [**vlan** *vlan-list*]

undo igmp-snooping fast-leave [**vlan** *vlan-list*]

デフォルト

ポート Quick Out 機能がオフになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*:指定された VLAN が設定されていることを示します。vlan-list は、1 つまたは複数の VLAN を表す VLAN リストで、vlan-list ={vlan-id [to vlan-id]}&<1-10>のように表示されます。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、すべての VLAN が設定されます。

説明

igmp-snooping fast-leave コマンドを使用して、ポートでポートファーストアウト機能を有効にします。

undo igmp-snooping fast-leave コマンドを使用して、ポートのポートファーストアウト機能をオフにします。

指定されたマルチキャストグループからの IGMP 離脱グループメッセージをホストから受信すると、対応する転送テーブルエントリのアウトポートリストからポートを直接削除するポートファーストアウト機能を有効にします。

このコマンドは、fast-leave コマンドと同じですが、スコープが異なります。IGMP-snooping view の下のグローバル設定はすべてのポートに対して有効であり、Interface view の下の設定は現在のポートに対してのみ有効であり、後者の設定は優先度が高くなります。

例

#VLAN 2 内のポート GigabitEthernet1/0/1 でポート Quick Out 機能を有効にします。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping fast-leave vlan 2
```

関連コマンド

- **fast-leave (IGMP-Snooping view)**

24.1.20 igmp-snooping general-query source-ip

Syntax

igmp-snooping general-query source-ip *ip-address*

undo igmp-snooping general-query source-ip

デフォルト

VLAN 内の IGMP ユニバーサルグループ照会メッセージの送信元 IP アドレスは、現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスがない場合は、0.0.0.0 が使用されます。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address:IGMP 汎用グループ照会メッセージの送信元 IP アドレスを示します。

説明

igmp-snooping general-query source-ip コマンドを使用して、IGMP ユニバーサルグループ照会メッセージの送信元 IP アドレスを設定します。

undo igmp-snooping general-query source-ip コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

例

#VLAN 2 で IGMP Snooping を有効にし、IGMP ユニバーサルグループクエリメッセージの送信元 IP アドレスを 10.1.1.1 に設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping general-query source-ip 10.1.1.1

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**

24.1.21 igmp-snooping group-limit

Syntax

igmp-snooping group-limit *limit* [**vlan** *vlan-list*]

undo igmp-snooping group-limit [**vlan** *vlan-list*]

デフォルト

ポートが参加するマルチキャストグループの最大数に制限はありません。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

limit:ポートが参加するマルチキャストグループの最大数を 0~4294967295 の範囲で指定します。

vlan *vlan-list*:指定された VLAN が設定されていることを示します。vlan-list は、1 つまたは複数の VLAN を表す VLAN リストで、vlan-list ={vlan-id [to vlan-id]}&<1-10>のように表示されます。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、すべての VLAN が設定されます。

説明

igmp-snooping group-limit コマンドを使用して、ポートが加入するマルチキャストグループの最大数を設定します。

undo igmp-snooping group-limit コマンドは、マルチキャストグループに参加するポートの最大数の制限を解除するために使用します。

このコマンドは、ダイナミックマルチキャストグループに対してのみ有効で、スタティックマルチキャストグループに対しては無効です。

例

#設定ポート GigabitEthernet1/0/1 VLAN 2 内で加入できるマルチキャストグループの最大数は 10 です。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-limit 10 vlan 2

24.1.22 igmp-snooping group-policy

Syntax

igmp-snooping group-policy *ipv4-acl-number* [**vlan** *vlan-list*]

undo igmp-snooping group-policy [**vlan** *vlan-list*]

デフォルト

マルチキャストグループフィルタが設定されていません。つまり、ホストは任意の正当なマルチキャストグループに参加できます。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number:IPv 4 基本 ACL または拡張 ACL の番号を 2000~3999 の範囲で指定します。ホストは、ACL ルールで許可されているマルチキャストグループにのみ参加できます。指定された ACL が存在しない場合、または ACL に有効なルールが設定されていない場合は、すべてのマルチキャストグループが除外されます。

vlan *vlan-list*:指定された VLAN が設定されていることを示します。vlan-list は、1 つまたは複数の VLAN を表す VLAN リストで、vlan-list ={vlan-id [to vlan-id]}&<1-10>のように表示されます。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、すべての VLAN が設定されます。

説明

igmp-snooping group-policy コマンドを使用して、ポートにマルチキャストグループフィルタを設定し、ホストが参加できるマルチキャストグループを制限します。

undo igmp-snooping group-policy コマンドを使用して、ポート上のマルチキャストグループフィルタを削除します。

このコマンドは、ダイナミックマルチキャストグループに対してのみ有効で、スタティックマルチキャストグループに対しては無効です。

このコマンドは、**group-policy** コマンドと同じですが、スコープが異なります。IGMP-snooping view の下のグローバル設定はすべてのポートに対して有効であり、Interface view の下の設定は現在のポートに対してのみ有効であり、後者の設定は優先度が高くなります。

IPv 4 の指定 ACL を使用する場合は、次の点に注意してください。

- IPv 4 ベース ACL の場合、ACL ルールの source パラメータは、IGMP メッセージのマルチキャストグループアドレスの範囲を指定するために使用され、source、fragment、time-range 以外のオプションのパラメータは無視されます。
- IPv 4 拡張 ACL の場合、ACL ルールの source パラメータは IGMP メッセージのマルチキャスト送信元アドレス(IGMPv1/v2 メッセージと、マルチキャスト送信元アドレスを持たない IS_EX/TO_EX タイプの IGMPv3 メッセージの場合、マルチキャスト送信元アドレスが 0.0.0.0 であるとします。)の範囲を指定し、destination パラメータはマルチキャストグループアドレスの範囲を指定します。source、destination、fragment、time-range 以外のオプションのパラメータは無視されます。
- ポートごとに異なる ACL ルールを異なる VLAN に設定できますが、同じ VLAN に設定された新しいルールが古いルールに置き換わります。

例

#ポート GigabitEthernet1/0/1 でマルチキャストグループフィルタを設定して、VLAN 2 内のホストがマルチキャストグループ 225.1.1.1 にのみ参加できるようにします。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

関連コマンド

- **group-policy (IGMP-Snooping view)**

24.1.23 igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *seconds*

undo igmp-snooping host-aging-time

デフォルト

ダイナミックメンバポートのエージングタイムは 260 秒です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds:ダイナミックメンバポートのエージングタイムを秒単位で 1~8097894 の範囲で指定します。

説明

VLAN 内のダイナミックメンバポートのエージングタイムを設定するには、**igmp-snooping host-aging-time** コマンドを使用します。

undo igmp-snooping host-aging-time コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

このコマンドは、host-aging-time コマンドと同じですが、範囲が異なります。IGMP-snooping view の下のグローバル設定はすべての VLAN で有効で、VLAN view の下の設定は現在の VLAN でのみ有効で、後者の設定は優先順位が高くなります。

マルチキャストグループメンバの誤った削除を避けるため、ダイナミックメンバポートのエージングタイムが、IGMP ユニバーサルグループクエリメッセージの送信間隔と IGMP ユニバーサルグループクエリの最大応答時間の合計よりも大きくなるように設定してください。ダイナミックメンバポートのエージングタイムは、IGMP ユニバーサルグループクエリメッセージの送信間隔と IGMP ユニバーサルグループクエリの最大応答時間の合計の 2 倍に設定することをお勧めします。

例

#VLAN 2 で IGMP Snooping を有効にし、ダイナミックメンバポートのエージングタイムを 300 秒に設定します。

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping host-aging-time 300
```

関連コマンド

- **enable (IGMP-Snooping view)**
- **host-aging-time (IGMP-Snooping view)**
- **igmp-snooping enable**

24.1.24 igmp-snooping host-join

Syntax

igmp-snooping host-join *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping host-join { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

デフォルト

マルチキャストグループまたはマルチキャストソースグループに参加するように、アナログホストが設定されていません。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-address:擬似ホストが参加するマルチキャストグループのアドレスを示し、224.0.1.0239.255.255.255 の範囲で値をとる。

source-ip *source-address*:擬似ホストが参加するマルチキャスト送信元のアドレスを示す。このパラメータが指定されている場合は、マルチキャストソースグループに参加します。このパラメータが指定されていない場合は、マルチキャストグループに参加します。このパラメータを使用してアナログホストを設定することは、IGMP Snooping リリース 3 でのみ有効です。

vlan *vlan-id*:指定された VLAN が設定されていることを示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。

all:すべてのマルチキャストグループとマルチキャストソースグループが設定されていることを示す。

説明

igmp-snooping host-join コマンドを使用して、マルチキャストグループまたはマルチキャストソースグループに参加するようにアナログホストを設定します。エミュレートされたホスト参加とは、レイヤ 2 デバイスのポートをマルチキャストグループのメンバとして設定することです。

undo igmp-snooping host-join コマンドを使用して、ホスト加入をエミュレートする設定を削除します。

静的メンバポートとは異なり、アナログホストが参加するように構成されたポートは、動的メンバポートとして、動的メンバポートのエージングプロセスに参加します。

エミュレートされたホストで使用される IGMP のバージョンは、IGMP Snooping のバージョンと同じです。

例

#ポート GigabitEthernet1/0/1 で、VLAN 2 内のマルチキャスト送信元グループ(1.1.1.1、232.1.1.1)へのアナログホストの参加を設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping host-join 232.1.1.1 source-ip 1.1.1.1 vlan 2

24.1.25 igmp-snooping last-member-query-interval

Syntax

igmp-snooping last-member-query-interval *interval*

undo igmp-snooping last-member-query-interval

デフォルト

IGMP 固有のグループクエリメッセージの送信間隔は 1 秒です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval:IGMP 特定グループクエリメッセージの送信間隔を示し、1~25 の範囲の値をとり、単位は秒である。

説明

igmp-snooping last-member-query-interval コマンドを使用して、VLAN 内で IGMP 固有のグループクエリメッセージの送信間隔を設定します。

undo igmp-snooping last-member-query-interval コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

このコマンドは、**last-member-query-interval** コマンドと同じですが、範囲が異なります。IGMP-snooping view の下のグローバル設定はすべての VLAN で有効で、VLAN view の下の設定は現在の VLAN でのみ有効で、後者の設定は優先順位が高くなります。

例

#VLAN 2 で IGMP Snooping を有効にし、IGMP の特定のグループクエリメッセージの送信間隔を 3 秒に設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping last-member-query-interval 3

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**
- **last-member-query-interval (IGMP-Snooping view)**

24.1.26 igmp-snooping leave source-ip

Syntax

igmp-snooping leave source-ip *ip-address*

undo igmp-snooping leave source-ip

デフォルト

VLAN 内では、IGMP 発信グループメッセージの送信元 IP アドレスは、現在の VLAN インタフェースの IP アドレスです。現在の VLAN インタフェースに IP アドレスがない場合は、0.0.0.0 が使用されます。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address:IGMP がグループメッセージの送信元 IP アドレスから離れることを示します。

説明

igmp-snooping leave source-ip コマンドは、IGMP がグループメッセージから離れるように設定するために使用する送信元 IP アドレスです。

undo igmp-snooping leave source-ip コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

例

#VLAN 2 内で IGMP Snooping を有効にし、IGMP がグループメッセージの送信元 IP アドレス 10.1.1.1 から離れるように設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping leave source-ip 10.1.1.1

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**

24.1.27 igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *seconds*

undo igmp-snooping max-response-time

デフォルト

IGMP ユニバーサルグループクエリの最大応答時間は 10 秒です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds:IGMP 汎用グループクエリの最大応答時間を秒単位で 1~3174 の範囲で指定します。

説明

VLAN 内の IGMP ユニバーサルグループクエリの最大応答時間を設定するには、**igmp-snooping max-response-time** コマンドを使用します。

undo igmp-snooping max-response-time コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

このコマンドは、max-response-time コマンドと同じですが、範囲が異なります。IGMP-snooping view の下のグローバル設定はすべての VLAN で有効で、VLAN view の下の設定は現在の VLAN でのみ有効で、後者の設定は優先順位が高くなります。

マルチキャストグループメンバの誤った削除を避けるには、IGMP 汎用グループクエリの最大応答時間が IGMP 汎用グループクエリメッセージの送信間隔より短いことを確認してください。そうでない場合、設定は有効になりますが、プロンプトが表示されます。

例

#VLAN 2 で IGMP Snooping を有効にし、IGMP ユニバーサルグループクエリの最大応答時間を 5 秒に設定します。

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping max-response-time 5
```

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**
- **igmp-snooping query-interval**
- **max-response-time (IGMP-Snooping view)**

24.1.28 igmp-snooping overflow-replace

Syntax

igmp-snooping overflow-replace [**vlan** *vlan-list*]

undo igmp-snooping overflow-replace [**vlan** *vlan-list*]

デフォルト

マルチキャストグループ置換機能がオフになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*:指定された VLAN が設定されていることを示します。vlan-list は、1 つまたは複数の VLAN を表す VLAN リストで、vlan-list ={vlan-id [to vlan-id]}&<1-10>のように表示されます。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、すべての VLAN が設定されます。

説明

igmp-snooping overflow-replace コマンドを使用して、ポートでマルチキャストグループ置換機能を有効にします。

undo igmp-snooping overflow-replace コマンドは、ポートでマルチキャストグループ置換機能を無効にするために使用されます。

このコマンドは、ダイナミックマルチキャストグループに対してのみ有効で、スタティックマルチキャストグループに対しては無効です。

このコマンドは、**overflow-replace** コマンドと同じですが、スコープが異なります。IGMP-snooping view の下のグローバル設定はすべてのポートに対して有効であり、Interface view の下の設定は現在のポートに対してのみ有効であり、後者の設定は優先度が高くなります。

例

#VLAN 2 内のポート GigabitEthernet1/0/1 でマルチキャストグループ置換機能を有効にします。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping overflow-replace vlan 2

関連コマンド

- **overflow-replace (IGMP-Snooping view)**

24.1.29 igmp-snooping querier

Syntax

igmp-snooping querier

undo igmp-snooping querier

デフォルト

IGMP Snooping クエリアが閉じています。

View

VLAN view

定義済みユーザロール

network-admin

説明

igmp-snooping querier コマンドは、IGMP Snooping クエリアを開くために使用します。

undo igmp-snooping querier コマンドは、IGMP Snooping クエリアを閉じるために使用します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

このコマンドがマルチキャスト VLAN のサブ VLAN 内で設定されている場合、そのサブ VLAN がマルチキャスト VLAN から削除されるまで、IGMP Snooping クエリアは有効になりません。

例

#VLAN 2 で IGMP Snooping を有効にし、IGMP Snooping クエリアを開きます。

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping querier
```

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**

24.1.30 igmp-snooping query-interval

Syntax

igmp-snooping query-interval *interval*

undo igmp-snooping query-interval

デフォルト

IGMP 汎用グループ照会メッセージの送信間隔は 125 秒です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interval:IGMP ユビキタスグループクエリーメッセージの送信間隔を示し、値の範囲は 2-31744,単位は秒である。

説明

igmp-snooping query-interval コマンドを使用して、VLAN 内の IGMP ユニバーサルグループ照会メッセージの送信間隔を設定します。

undo igmp-snooping query-interval コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

マルチキャストグループメンバの誤った削除を回避するには、IGMP 汎用グループクエリメッセージの送信間隔が IGMP 汎用グループクエリの最大応答時間よりも長いことを確認してください。そうでない場合、設定は有効になりますが、プロンプトが表示されます。

例

#VLAN 2 で IGMP Snooping を有効にし、IGMP ユニバーサルグループクエリメッセージの送信間隔を 20 秒に設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping query-interval 20

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**
- **igmp-snooping max-response-time**
- **igmp-snooping querier**
- **max-response-time**

24.1.31 igmp-snooping report source-ip

Syntax

igmp-snooping report source-ip *ip-address*

undo igmp-snooping report source-ip

デフォルト

VLAN 内では、IGMP メンバシップは、メッセージの送信元 IP アドレスが現在の VLAN インタフェースの IP アドレスであることを報告します。現在の VLAN インタフェースに IP アドレスがない場合は、0.0.0.0 が使用されます。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address:IGMP メンバシップレポートメッセージの送信元 IP アドレスを示します。

説明

igmp-snooping report source-ip コマンドを使用して、IGMP メンバシップレポートメッセージの送信元 IP アドレスを設定します。

undo igmp-snooping report source-ip コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

例

#VLAN 2 で IGMP Snooping を有効にし、IGMP メンバシップレポートメッセージの送信元 IP アドレスを 10.1.1.1 に設定します。

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping report source-ip 10.1.1.1
```

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**

24.1.32 igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *seconds*

undo igmp-snooping router-aging-time

デフォルト

ダイナミックルータポートのエージングタイムは 260 秒です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

seconds:ダイナミックルータポートのエージング時間を秒単位で 1~8097894 の範囲で指定します。

説明

VLAN 内のダイナミックルータポートのエージングタイムを設定するには、**igmp-snooping router-aging-time** コマンドを使用します。

undo igmp-snooping router-aging-time コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

このコマンドは、**router-aging-time** コマンドと同じですが、範囲が異なります。IGMP-snooping view の下のグローバル設定はすべての VLAN で有効で、VLAN view の下の設定は現在の VLAN でのみ有効で、後者の設定は優先順位が高くなります。

例

#VLAN 2 で IGMP Snooping を有効にし、ダイナミックルータポートのエージングタイムを 100 秒に設定します。

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping router-aging-time 100
```

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**
- **router-aging-time (IGMP-Snooping view)**

24.1.33 igmp-snooping special-query source-ip

Syntax

igmp-snooping special-query source-ip *ip-address*

undo igmp-snooping special-query source-ip

デフォルト

VLAN 内で IGMP 汎用グループクエリメッセージを受信した場合、IGMP 特定グループクエリメッセージの送信元 IP アドレスとして、その送信元 IP アドレスが使用されます。それ以外の場合は、現在の VLAN インタフェースの IP アドレスが使用されます。現在の VLAN インタフェースに IP アドレスがない場合は、0.0.0.0 が使用されます。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

ip-address:IGMP 特定グループのクエリメッセージの送信元 IP アドレスを示します。

説明

igmp-snooping special-query source-ip コマンドを使用して、IGMP 特定グループのクエリメッセージの送信元 IP アドレスを設定します。

undo igmp-snooping special-query source-ip コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

例

#VLAN 2 で IGMP Snooping を有効にし、IGMP の特定のグループクエリメッセージの送信元 IP アドレスを 10.1.1.1 に設定します。

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping special-query source-ip 10.1.1.1
```

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**

24.1.34 igmp-snooping static-group

Syntax

igmp-snooping static-group *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*

undo igmp-snooping static-group { *group-address* [**source-ip** *source-address*] **vlan** *vlan-id* | **all** }

デフォルト

ポートは静的メンバポートではありません。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

group-address: 静的に加入するマルチキャストグループアドレスを表し、224.0.1.0239.255.255.255 の範囲の値をとる。

source-ip *source-address*:静的に参加するマルチキャスト送信元アドレスを示します。このパラメータが指定されている場合は、マルチキャストソースグループに参加します。このパラメータが指定されていない場合は、マルチキャストグループに参加します。このパラメータで静的なメンバポートを設定することは、IGMP Snooping リリース 3 でのみ有効です。

vlan *vlan-id*:指定された VLAN が設定されていることを示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。

all:すべてのマルチキャストグループとマルチキャストソースグループが設定されていることを示す。

説明

igmp-snooping static-group コマンドを使用して、スタティックメンバポートを設定します。つまり、マルチキャストグループまたはマルチキャスト送信元グループにスタティックに加入するようにポートを設定します。

スタティックメンバポートの設定を削除するには、**undo igmp-snooping static-group** コマンドを使用します。

例

#ポート GigabitEthernet1/0/1 を、VLAN 2 内のマルチキャスト送信元グループ(1.1.1.1、225.0.0.1)のスタティックメンバポートとして設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3
[Sysname-vlan2] quit
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-group 225.0.0.1 source-ip 1.1.1.1 vlan 2

24.1.35 igmp-snooping static-router-port

Syntax

igmp-snooping static-router-port vlan *vlan-id*

undo igmp-snooping static-router-port { **all** | **vlan** *vlan-id* }

デフォルト

ポートはスタティックルータポートではありません。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

all:すべての VLAN が設定されていることを示します。

vlan *vlan-id*:指定された VLAN が設定されていることを示します。vlan-id は VLAN の番号で、範囲は 1~4094 です。

説明

スタティックルータポートを設定するには、**igmp-snooping static-router-port** コマンドを使用します。

スタティックルータポートの設定を削除するには、**undo igmp-snooping static-router-port** コマンドを使用します。

例

#ポート GigabitEthernet1/0/1 を VLAN 2 内のスタティックルータポートとして設定します。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping static-router-port vlan 2

24.1.36 igmp-snooping version

Syntax

igmp-snooping version *version-number*

undo igmp-snooping version

デフォルト

VLAN 内 IGMP Snooping のバージョンは 2 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

version-number:IGMP Snooping のバージョン番号を表し、2~3 の値を取ります。

説明

VLAN 内でバージョン IGMP Snooping を設定するには、**igmp-snooping version** コマンドを使用します。

undo igmp-snooping version コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定する前に、VLAN 内で IGMP Snooping をイネーブルにする必要があります。

VLAN ベースの設定の場合、このコマンドの機能は version コマンドと同じですが、範囲が異なります。IGMP-snooping view では指定された VLAN を設定でき、VLAN view では現在の VLAN のみを設定できます。設定の優先順位は同じです。

例

#VLAN 2 で IGMP Snooping を有効にし、その VLAN で IGMP Snooping バージョン 3 を設定します。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping version 3

関連コマンド

- **enable (IGMP-Snooping view)**
- **igmp-snooping enable**
- **version (IGMP-Snooping view)**

24.1.37 last-member-query-interval (IGMP-Snooping view)

Syntax

last-member-query-interval *interval*

undo last-member-query-interval

デフォルト

IGMP 固有のグループクエリメッセージの送信間隔は 1 秒です。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

interval:IGMP 特定グループクエリメッセージの送信間隔を示し、125 の範囲の値をとり、単位は秒である。

説明

last-member-query-interval コマンドを使用して、IGMP 特定のグループクエリメッセージの送信間隔をグローバルに設定します。

undo last-member-query-interval コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、**igmp-snooping last-member-query-interval** コマンドと同じですが、範囲が異なります。IGMP-snooping view の下のグローバル設定はすべての VLAN で有効で、VLAN view の下の設定は現在の VLAN でのみ有効で、後者の設定は優先順位が高くなります。

例

#グローバル設定 IGMP 特定のグループクエリメッセージの送信間隔は 3 秒です。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] last-member-query-interval 3

関連コマンド

- **igmp-snooping last-member-query-interval**

24.1.38 max-response-time (IGMP-Snooping view)

Syntax

max-response-time *seconds*

undo max-response-time

デフォルト

IGMP ユニバーサルグループクエリの最大応答時間は 10 秒です。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds:IGMP 汎用グループクエリの最大応答時間を秒単位で 1~3174 の範囲で指定します。

説明

max-response-time コマンドを使用して、IGMP ユニバーサルグループクエリの最大応答時間をグローバルに設定します。

undo max-response-time コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、**igmp-snooping max-response-time** コマンドと同じですが、範囲が異なります。IGMP-snooping view の下のグローバル設定はすべての VLAN で有効で、VLAN view の下の設定は現在の VLAN でのみ有効で、後者の設定は優先順位が高くなります。

マルチキャストグループメンバの誤った削除を避けるには、IGMP 汎用グループクエリの最大応答時間が IGMP 汎用グループクエリメッセージの送信間隔より短いことを確認してください。そうでない場合、設定は有効になりますが、プロンプトが表示されます。

例

#グローバル設定 IGMP ユニバーサルグループクエリの最大応答時間は 5 秒です。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] max-response-time 5

関連コマンド

- **igmp-snooping max-response-time**
- **igmp-snooping query-interval**

24.1.39 overflow-replace (IGMP-Snooping view)

Syntax

overflow-replace [**vlan** *vlan-list*]

undo overflow-replace [**vlan** *vlan-list*]

デフォルト

マルチキャストグループ置換機能がオフになっています。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-list*:指定された VLAN が設定されていることを示します。vlan-list は、1 つまたは複数の VLAN を表す VLAN リストで、vlan-list ={vlan-id [to vlan-id]}&<1-10>のように表示されます。ここで、vlan-id は VLAN の番号で、範囲は 1~4094 です。&<1-10>は、前のパラメータが最大 10 回入力できることを示します。このパラメータが指定されていない場合は、すべての VLAN が設定されます。

説明

overflow-replace コマンドは、マルチキャストグループ置換機能をグローバルに起動するために使用します。

undo overflow-replace コマンドは、マルチキャストグループ置換機能をグローバルに停止するために使用します。

このコマンドは、ダイナミックマルチキャストグループに対してのみ有効で、スタティックマルチキャストグループに対しては無効です。

このコマンドは、**igmp-snooping overflow-replace** コマンドと同じですが、スコープが異なります。IGMP-snooping view の下のグローバル設定はすべてのポートに対して有効であり、Interface view の下の設定は現在のポートに対してのみ有効であり、後者の設定は優先度が高くなります。

例

#VLAN 2 内のマルチキャストグループ置換機能をグローバルに有効にします。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] overflow-replace vlan 2

関連コマンド

- **igmp-snooping overflow-replace**

24.1.40 report-aggregation (IGMP-Snooping view)

Syntax

report-aggregation

undo report-aggregation

デフォルト

IGMP メンバシップは、メッセージ抑制機能がオンになっていることを報告します。

View

IGMP-snooping view

定義済みユーザロール

network-admin

説明

report-aggregation コマンドを使用して、IGMP メンバシップレポートメッセージ抑制機能を有効にします。

undo report-aggregation コマンドを使用して、IGMP メンバシップレポートメッセージ抑制機能を無効にします。

例

#IGMP メンバシップレポートメッセージ抑制機能をオフにします。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] undo report-aggregation

24.1.41 reset igmp-snooping group

Syntax

reset igmp-snooping group { *group-address* [*source-address*] | **all** } [**vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

group-address:指定されたマルチキャストグループの情報をクリアします。範囲は 224.0.1.0~239.255.255.255 です。

source-address:指定されたマルチキャストソースの情報をクリアします。このパラメータが指定されていない場合、すべてのマルチキャストソースの情報がクリアされます。

all:すべてのマルチキャストグループの情報をクリアします。

vlan *vlan-id*:指定した VLAN 内の情報をクリアします。vlan-id は VLAN の番号で、範囲は 1~4094 です。このパラメータを指定しないと、すべての VLAN の情報がクリアされます。

説明

reset igmp-snooping group コマンドは、ダイナミック IGMP Snooping マルチキャストグループの情報をクリアするために使用されます。

例

#すべてのダイナミック IGMP Snooping マルチキャストグループの情報をクリアします。

<Sysname> reset igmp-snooping group all

関連コマンド

- **display igmp-snooping group**

24.1.42 reset igmp-snooping router-port

Syntax

reset igmp-snooping router-port { **all** | **vlan** *vlan-id* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all:すべてのダイナミックルータポートの情報をクリアします。

vlan *vlan-id*:指定した VLAN 内の情報をクリアします。vlan-id は VLAN の番号で、範囲は 1~4094 です。このパラメータを指定しないと、すべての VLAN の情報がクリアされます。

説明

reset igmp-snooping router-port コマンドを使用して、ダイナミックルータポートの情報をクリアします。

例

#すべてのダイナミックルータポートの情報をクリアします。

<Sysname> reset igmp-snooping router-port all

関連コマンド

- **display igmp-snooping router-port**

24.1.43 reset igmp-snooping statistics

Syntax

reset igmp-snooping statistics

View

User view

定義済みユーザロール

network-admin

説明

reset igmp-snooping statistics コマンドは、IGMP Snooping が受信する IGMP メッセージの統計情報をクリアするために使用されます。

例

#IGMP Snooping が受信する IGMP メッセージの統計情報をクリアします。

<Sysname> reset igmp-snooping statistics

関連コマンド

- **display igmp-snooping statistics**

24.1.44 router-aging-time (IGMP-Snooping view)

Syntax

router-aging-time *seconds*

undo router-aging-time

デフォルト

ダイナミックルータポートのエージングタイムは 260 秒です。

View

IGMP-snooping view

定義済みユーザロール

network-admin

パラメータ

seconds:ダイナミックルータポートのエージング時間を秒単位で 1~8097894 の範囲で指定します。

説明

ダイナミックルータポートのエージングタイムをグローバルに設定するには、**router-aging-time** コマンドを使用します。

undo router-aging-time コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、**igmp-snooping router-aging-time** コマンドと同じですが、範囲が異なります。IGMP-snooping view の下のグローバル設定はすべての VLAN で有効で、VLAN view の下の設定は現在の VLAN でのみ有効で、後者の設定は優先順位が高くなります。

例

#グローバル設定ダイナミックルータポートのエージングタイムは 100 秒です。

<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] router-aging-time 100

関連コマンド

- **igmp-snooping router-aging-time**

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

6.WLAN アクセス

本マニュアルは以下に示す章で構成されています。

01-WLAN アクセス

目次

このセクションのページは **6-x-x** です。

1 章 WLAN アクセス 1-1
1.1 WLAN アクセス設定コマンド 1-1
1.1.1 access-control acl 1-1
1.1.2 beacon ssid-hide 1-3
1.1.3 broadcast-probe reply 1-3
1.1.4 client association-location 1-5
1.1.5 client forwarding-location 1-5
1.1.6 client frame-format 1-6
1.1.7 client idle-timeout 1-7
1.1.8 client keep-alive 1-8
1.1.9 client keep-alive interval 1-9
1.1.10 client max-count 1-10
1.1.11 client preferred-vlan authorized 1-11
1.1.12 client vlan-alloc 1-12
1.1.13 description 1-13
1.1.14 display wlan blacklist 1-14
1.1.15 display wlan bss 1-15
1.1.16 display wlan client 1-17
1.1.17 display wlan client failure 1-24
1.1.18 display wlan client status 1-25
1.1.19 display wlan service-template 1-28
1.1.20 display wlan statistics client 1-34
1.1.21 display wlan statistics connect-history 1-35
1.1.22 display wlan statistics service-template 1-36
1.1.23 display wlan whitelist 1-38
1.1.24 nas-id 1-38
1.1.25 nas-port-id 1-40
1.1.26 reset wlan client 1-41
1.1.27 reset wlan dynamic-blacklist 1-41
1.1.28 reset wlan statistics client 1-42
1.1.29 reset wlan statistics service-template 1-43
1.1.30 service-template 1-43
1.1.31 service-template enable 1-45
1.1.32 snmp-agent trap enable wlan client 1-45
1.1.33 ssid 1-46
1.1.34 unknown-client 1-47

1.1.35 vlan 1-48
1.1.36 wlan client failure history aging 1-48
1.1.37 wlan client reauthentication-period 1-49
1.1.38 wlan dynamic-blacklist active-on-ap 1-50
1.1.39 wlan dynamic-blacklist lifetime 1-51
1.1.40 wlan link-test 1-52
1.1.41 wlan nas-port-id format 1-54
1.1.42 wlan permit-ssid 1-55
1.1.43 wlan service-template 1-56
1.1.44 wlan static-blacklist mac-address 1-57
1.1.45 wlan whitelist mac-address 1-58

1章 WLAN アクセス

1.1 WLANアクセス設定コマンド

1.1.1 access-control acl

Syntax

access-control acl *acl-number* **[permit-remote-ap]**

undo access-control acl

デフォルト

ACL の指定はありません。

View

AP view

Service template view

定義済みユーザロール

network-admin

パラメータ

acl-number:レイヤ 2 ACL の番号を 4000 から 4999 の範囲で指定します。

permit-remote-ap:リモート AP で許可ルールを有効にできます。このキーワードを指定しない場合、ACL はリモート AP に適用されません。

説明

access-control acl コマンドは ACL ベースのアクセス制御の ACL を指定します。

undo access-control acl コマンドは設定をデフォルトに戻します。

この機能は、指定された ACL ルールを使用してクライアントアクセスを制御します。デバイスは、アソシエーション要求を受信すると、次のアクションを実行します。

- クライアントの MAC アドレスがルールの MAC アドレス属性または MAC アドレス OUI 属性と一致し、ルールアクションが許可されている場合に、クライアントが WLAN にアクセスできるようにします。複数のクライアントが OUI 属性と一致する場合、これらのすべてのクライアントが WLAN にアクセスできるようになります。
- 一致するものが見つからない場合、または一致したルールに deny ステートメントがある場合、クライアントの WLAN へのアクセスを拒否します。

この機能を設定する場合は、次の制限とガイドラインに従ってください。

- 指定した ACL に deny ステートメントが含まれている場合は、すべてのクライアントを許可するようにACLのpermitステートメントを設定します。これを行わないと、クライアントはオンラインにできません。
- ACL ベースのアクセスコントロール設定は、ホワイトリストおよびブラックリスト設定よりも優先されます。
- 指定できる ACL は 1 つだけです。このコマンドを複数回実行すると、最新の設定が有効になります。
- AP view の設定は、Service template view の設定よりも優先されます。

リモート AP 機能を有効にし、ACL に **permit-remote-ap** キーワードを指定すると、AC は許可ルールに一致するオンラインクライアントのキャッシュエントリを AP と同期します。AP がリモート状態になると、キャッシュエントリ内のクライアントだけがネットワークにアクセスできます。

例

MAC アドレスが 000e-35b2-000e のクライアントと指定された OUI のクライアントを許可する ACL 4000 を作成し、ACL ルールを作成します。サービステンプレート service1 に ACL 4000 を指定します。

<Sysname> system-view

[Sysname] acl mac 4000

[Sysname-acl-mac-4000] rule 0 permit source-mac 000e-35b2-000e ffff-ffff-ffff

[Sysname-acl-mac-4000] rule 1 permit source-mac 000e-35b2-000f ffff-ff00-0000

[Sysname-acl-mac-4000] rule 2 deny

[Sysname-acl-mac-4000] quit

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] access-control acl 4000

MAC アドレスが 000e-35b2-000e のクライアントと指定された OUI のクライアントを許可する ACL 4000 を作成し、ACL ルールを作成します。AP ap1 に ACL 4000 を指定します。

<Sysname> system-view

[Sysname] acl mac 4000

[Sysname-acl-mac-4000] rule 0 permit source-mac 000e-35b2-000e ffff-ffff-ffff

[Sysname-acl-mac-4000] rule 1 permit source-mac 000e-35b2-000f ffff-ff00-0000

[Sysname-acl-mac-4000] rule 2 deny

[Sysname-acl-mac-4000] quit

[Sysname] wlan ap ap1 model WA6320

[Sysname-wlan-ap-ap1] access-control acl 4000

1.1.2 beacon ssid-hide

Syntax

beacon ssid-hide

undo beacon ssid-hide

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

beacon ssid-hide コマンドは SSID ステルスを有効にします。

undo beacon ssid-hide コマンドはデフォルトに戻します。

このコマンドを設定すると、無線がビーコンフレーム内で SSID を伝送しないようになり、指定したサービステンプレートが無線にバインドされた後にプローブ要求に応答しなくなります。

⚠ **注意：**

6GHz 帯の SSID で SSID ステルスを有効にすると接続できない端末があります。
6GHz 帯で利用するサービステンプレートでは SSID ステルスを有効にしないでください。

例

ビーコンフレームで SSID のアドバタイズを無効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] beacon ssid-hide

1.1.3 broadcast-probe reply

Syntax

broadcast-probe reply { **disable** | **enable** [**rssi-threshold** *rssi-value*] } [**frequency-band** { **2.4** | **5** }]

undo broadcast-probe reply

デフォルト

AP view：AP group view の設定を使用します。

AP group view：ブロードキャストプローブ要求に応答します。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold *rssi-value*: RSSI しきい値を 1 から 100 の範囲で指定します。このオプションを指定しない場合、AP は任意の RSSI でブロードキャストプローブ要求に応答できます。

frequency-band： 周波数帯域を指定します。このキーワードを指定しない場合、5 GHz と 2.4 GHz の両方の帯域で受信したブロードキャストプローブ要求に AP が応答できるようになります。

2.4:動作周波数帯は 2.4 GHz。

5:動作周波数帯は 5 GHz。

説明

broadcast-probe reply enable コマンドは AP のブロードキャストプローブ要求への応答を有効にします。

broadcast-probe reply disable コマンドは AP のブロードキャストプローブ要求への応答を無効にします。

undo broadcast-probe reply コマンドはデフォルトに戻します。

ブロードキャストプローブ要求には SSID は含まれません。AP はブロードキャストプローブ要求を受信すると、AP のサービス情報を含んだプローブ応答を返信します。ユニキャストプローブ要求を送信するクライアントが AP に接続することができるようにするには、AP がブロードキャストプローブ要求に応答しないようにします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 をブロードキャストプローブ要求に応答しないようにします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] broadcast-probe reply disable

AP グループ group1 の AP をブロードキャストプローブ要求に応答しないようにします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] broadcast-probe reply disable

1.1.4 client association-location

Syntax

client association-location { **ac** | **ap** }

undo client association-location

デフォルト

AC

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ac:クライアントのアソシエーション位置は AC 上です。

ap: クライアントのアソシエーション位置は AP 上です。

説明

client association-location コマンドを使用して、クライアントアソシエーションの位置を設定します。

undo client association-location コマンドはデフォルト戻します。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

例

#AC 上のクライアントアソシエーションの位置を設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] client association-location ac

1.1.5 client forwarding-location

Syntax

client forwarding-location { **ac** | **ap** }

undo client forwarding-location

デフォルト

AP はクライアントデータ トラフィックを転送します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ac : AC がクライアントデータ トラフィックを転送します。

ap : AP がクライアントデータ トラフィックを転送します。

説明

client forwarding-location コマンドはクライアントデータ トラフィックフォワーダを指定します。

undo client forwarding-location コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレート が無効であることを確認してください。

AC トラフィックがクライアントトラフィックフォワーダとして設定されている場合、クライアントのトラフィック転送が有効になっていることを確認してください。

例

#パケット転送先を AP に設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

1.1.6 client frame-format

Syntax

client frame-format { **dot3** | **dot11** }

undo client frame-format

デフォルト

クライアントデータフレームは 802.3 形式でカプセル化されます。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot3: 802.3 形式を指定します。

dot11: 802.11 形式を指定します。

説明

client frame-format コマンドはクライアントデータフレームのカプセル化モードを設定します。

undo client frame-format コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートが無効であることを確認してください。

このコマンドは、中央転送モードでのみ有効です。

例

#クライアントデータフレームを 802.11 フォーマットでカプセル化します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client frame-format dot11

関連コマンド

- client forwarding-location

1.1.7 client idle-timeout

Syntax

client idle-timeout *timeout*

undo client idle-timeout

デフォルト

AP view：AP group view の設定を使用します。

AP group view：300 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

timeout: クライアントアイドルタイムアウト時間を指定します。設定範囲は 60～86400 秒です。

説明

client idle-timeout コマンドはクライアントアイドルタイムアウトタイマーを設定します。

undo client idle-timeout コマンドはデフォルトに戻します。

クライアントアイドルタイムアウト時間内にオンラインクライアントが接続した AP にフレームを送信しない場合、AP はクライアントをログオフします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 のクライアントアイドルタイムアウト時間を 2000 秒に設定します。

<sysname> system-view

[sysname] wlan ap ap1 model WA6320

[sysname-wlan-ap-ap1] client idle-timeout 2000

AP group group1 のクライアントアイドルタイムアウト時間を 2000 秒に設定します。

<Sysname> system-view

[Sysname] wlan ap-group group1

[Sysname-wlan-ap-group-group1] client idle-timeout 2000

1.1.8 client keep-alive

Syntax

client keep-alive { **disable** | **enable** }

undo client keep-alive

デフォルト

AP view： AP group view の設定を使用します。

AP group view：無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: クライアントキープアライブを無効にします。

enable: クライアントキープアライブを有効にします。

説明

client keep-alive enable コマンドはクライアントキープアライブを有効にします。

client keep-alive disable コマンドはクライアントキープアライブを無効にします。

undo client keep-alive コマンドはデフォルトに戻します。

AP は、クライアントにキープアライブ間隔でキープアライブパケットを送信し、クライアントがオンラインかどうかを確認できます。キープアライブ間隔 3 回でクライアントからの応答を受信しない場合、AP はクライアントをログオフします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 のクライアントキープアライブを有効にします。

<Sysname> system-view

[Sysname] wlan ap ap1 model WA6320

[Sysname-wlan-ap-ap1] client keep-alive enable

#AP group group1 のクライアントキープアライブを有効にします。

<Sysname> system-view

[Sysname] wlan ap-group group1

[Sysname-wlan-ap-group-group1] client keep-alive enable

関連コマンド

- client keep-alive interval

1.1.9 client keep-alive interval

Syntax

client keep-alive interval *interval*

undo client keep-alive interval

デフォルト

AP view：AP group view の設定を使用します。

AP group view：300 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: クライアントのキープアライブ間隔を指定します。設定範囲は 3～1800 秒です。

説明

client keep-alive interval コマンドはクライアントキープアライブ間隔を設定します。

undo client keep-alive interval コマンドはデフォルトに戻します。

このコマンドを実行する前に、クライアントキープアライブを有効にしてください。

AP は、クライアントにキープアライブ間隔でキープアライブパケットを送信し、クライアントがオンラインかどうかを確認できます。キープアライブ間隔 3 回でクライアントからの応答を受信しない場合、AP はクライアントをログオフします。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 のキープアライブ間隔を 20 秒に設定します。

<Sysname> system-view

[Sysname] wlan ap ap1 model WA6320

[Sysname-wlan-ap-ap1] client keep-alive interval 20

AP group group1 のキープアライブ間隔を 20 秒に設定します。

<Sysname> system-view

[Sysname] wlan ap-group group1

[Sysname-wlan-ap-group-group1] client keep-alive interval 20

関連コマンド

- client keep-alive enable

1.1.10 client max-count

Syntax

client max-count *max-number*

undo client max-count

デフォルト

制限なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

max-number: 1～512 の範囲内のクライアントの最大数を指定します。

説明

client max-count コマンドはサービステンプレートに関連するクライアントの最大数を設定します。

undo client max-count コマンドはデフォルトに戻します。

この機能を設定すると、新しいクライアントは無線から WLAN にアクセスできなくなり、無線で最大数に達すると SSID は非表示になります。

例

サービステンプレート service1 の関連するクライアントの最大数を 38 に設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] client max-count 38

関連コマンド

- beacon ssid-hide

1.1.11 client preferred-vlan authorized

Syntax

client preferred-vlan authorized

undo client preferred-vlan authorized

デフォルト

クライアントは許可 VLAN を優先的に使用します。

View

Service template view

定義済みユーザロール

network-admin

説明

client preferred-vlan authorized コマンドはローミング後に許可 VLAN を優先するようにクライアントを設定します。

undo client preferred-vlan authorized コマンドはローミング後にクライアント VLAN が変更されないように設定します。

この機能は 802.1X および MAC 認証クライアントでのみ有効です。

通常、クライアントの VLAN は、クライアントのローミング後も変更されません。ただし、クライアントが別の AP にローミングした後に QMC で設定されたセキュリティ警告をトリガすると、ユーザアイソレーションのために発行された許可 VLAN が有効になります。

例

#許可 VLAN を優先するようにクライアントを設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] client preferred-vlan authorized

1.1.12 client vlan-alloc

Syntax

client vlan-alloc { **dynamic** | **static** | **static-compatible** }

undo client vlan-alloc

デフォルト

dynamic

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dynamic: ダイナミック VLAN 割り当てを指定します。

static: スタティック VLAN 割り当てを指定します。

static-compatible: スタティックに互換性のある VLAN 割り当てを指定します。

説明

client vlan-alloc コマンドはクライアントの VLAN 割り当て方法を指定します。

undo client vlan-alloc コマンドはデフォルトに戻します。

クライアントが初めてオンラインになると、無線はランダムな VLAN を割り当てます。クライアントが再びオンラインになると、クライアントに割り当てられた VLAN は割り当て方法に依存します。

- **Static allocation**:クライアントは、割り当てられた VLAN を継承します。IP アドレスのリースが期限切れになっていない場合、クライアントは同じ IP アドレスを使用します。この方法は、IP アドレスを節約するのに役立ちます。
- **Dynamic allocation**:クライアントに VLAN が再割り当てされます。この方法では、すべての VLAN のクライアントで負荷を分散させます。
- **Static-compatible allocation**:スタティックに割り当てられたバージョン ComwareV5 の AC デバイスとバージョン ComwareV7 の AC 間をローミングするときに、クライアントに同じ VLAN が割り当てられます。

例

クライアントの VLAN 割り当て方法をダイナミックに指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] client vlan-alloc dynamic

関連コマンド

- service-template

1.1.13 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

text: description 名を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

description コマンドはサービステンプレートの説明を構成します。

undo description コマンドはデフォルトに戻します。

例

サービステンプレート service1 に description 名 wlanst を指定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] description wlanst

1.1.14 display wlan blacklist

Syntax

display wlan blacklist { **dynamic** | **static** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: ダイナミックブラックリストを指定します。

static:スタティックブラックリストを指定します。

説明

display wlan blacklist コマンドはブラックリストエントリを表示します。

例

スタティックブラックリストエントリを表示します。

<Sysname> display wlan blacklist static

```
Total number of clients:3
MAC addresses:
000 e-35b2-000e
0019-5 b8e-b709
001 c-f0bf-9c92
```

#ダイナミックブラックリストを表示します。

<Sysname> display wlan blacklist dynamic

```
Total number of clients:3
MAC addressAPIDRIDLifetime (s)Duration (hh:mm:ss)
000 f-e2cc-00011130000:02:11
000 f-e2cc-00022130000:01:17
000 f-e2cc-00033130000:02:08
```

表 1-1 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
APID	不正クライアントが検出されたAPのシリアル番号
RID	不正クライアントが検出されたAPのRadio ID
Lifetime (s)	ダイナミックブラックリストエントリの経過時間 (秒)
Duration (hh:mm:ss)	ダイナミックブラックリストエントリの存続時間

1.1.15 display wlan bss

Syntax

display wlan bss { **all** | **ap** *ap-name* | **bssid** *bssid* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての BSS を表示します。

ap *ap-name*: AP 名を 1～64 文字の文字列で指定します。大文字と小文字を区別します。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（ - ）を使用できます。

bssid *bssid*: BSS を ID で指定します。ID は、48 ビットの 16 進数で H-H-H の形式で指定してください。

verbose: 詳細な BSS 情報を表示します。 このキーワードを指定しない場合、BSS 情報の概要を表示します。

説明

display wlan bss コマンドは BSS（Basic Service Set）情報を表示します。

例

すべての BSS の簡潔な情報を表示します。

<AC> display wlan bss all

```
Current BSS number: 4
Max BSS number: 6144
Bound BSS number: 5
AP name               RID  SSID                      BSSID
```

```
ap1                  1    SSID1                    001c-f08f-f804
ap1                  2    SSID1                    001c-f08f-f806
ap2                  1    SSID1                    001c-f0bf-9c92
ap2                  2    SSID1                    001c-f0bf-9c94
```

表 1-2 コマンド出力

フィールド	説明
Current BSS number	現在生成されているBSSの数
Max BSS number	サポートされているBSSの最大数
Bind BSS number	Radioにバインドされたサービステンプレートで生成されるBSSの数(生成可能なBSSの数が、サポートされているBSSの最大数を超える可能性があります。)

#メンバーデバイス 1 の BSSID が 001 c-f08f-f804 である BSS の詳細を表示します。

<Sysname> display wlan bss bssid 001c-f08f-f804 slot 1 verbose

```
AP name                    : ap1
BSSID                      : 001c-f08f-f804
Radio ID                   : 1
Service template name        : servcie1
SSID                       : SSID1
VLAN ID                    : 1
AKM mode                   : Not configured
User authentication mode     : Bypas
```

表 1-3 コマンド出力

フィールド	説明
AKM mode	認証およびキー管理モード: ● 802.1 X ● PSK ● Not configured:認証およびキー管理モードが設定されていません
User authentication mode	ユーザ認証モード: ● Bypass:ユーザ認証を行わない ● MAC ● 802.1 X ● OUI

1.1.16 display wlan client

🕮 メモ：

frequency-band 6 のパラメータは、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

Syntax

display wlan client [**ap** *ap-name* [**radio** *radio-id*] | **mac-address**

mac-address | **service-template** *service-template-name* | **frequency-band** { **2.4** | **5**

| **6** }] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: 指定した AP に接続されているクライアントに関する情報を表示します。AP 名は、1～64 文字の文字列です。大文字と小文字を区別しません。文字列には、文字、数字、アンダースコア（_）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

radio *radio-id*: 指定した無線に接続されているクライアントに関する情報を表示します。*radio-id* の範囲は、デバイスモデルによって異なります。このオプションを指定しないと、指定した AP に接続されているすべてのクライアントに関する情報が表示されます。

mac-address *mac-address*: クライアントを MAC アドレスで指定します。

service-template *service-template-name*: 指定したサービステンプレートに関連付けられているクライアントに関する情報を表示します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

frequency-band: 指定されたバンドで作業しているクライアントに関する情報を表示します。

2.4: 2.4GHz 帯を指定します。

5: 5GHz 帯を指定します。

6: 6GHz 帯を指定します。

verbose: 詳細なクライアント情報を表示します。このキーワードを指定しない場合、クライアント情報の概要を表示します。

説明

display wlan client コマンドはクライアント情報を表示します。

例

すべてのクライアントに関する簡潔なクライアント情報を表示します。

<Sysname> display wlan client

```
Total number of clients: 3
MAC address    Username          AP name           R IP address      VLAN
000f-e265-6400    N/A               ap1               1 1.1.1.1         100
000f-e265-6401    user              ap2               1 3.0.0.3          200
84db-ac14-dd08    N/A               ap1               1 5.5.5.3          1
```

表 1-4 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
Username	クライアントのユーザ名は、クライアントが802.1 X認証またはMACアドレス認証を行っていれば認証に使用したユーザ名を表示し、クライアントが802.1 X認証またはMACアドレス認証を行っていなければN/Aを表示します。 クライアントがPortal認証を使用している場合、Usernameフィールドにはクライアントの Portalユーザ名は表示されず、N/Aと表示されます。
AP name	クライアント関連APの名前
RID	クライアント関連Radio ID
IP address	クライアントのIPv 4アドレス
VLAN ID	クライアントが属するVLAN

すべてのクライアントに関する詳細なクライアント情報を表示します。

<Sysname> display wlan client mac-address 000f-e265-6400 verbose

Total number of clients: 1

MAC address : 000f-e265-6400

IPv4 address : 10.1.1.114

IPv6 address : 2001::1234:5678:0102:0304

Username : N/A

AID : 1

AP ID : 1

AP name : ap1

Radio ID : 1

Channel : 36

SSID : office
BSSID : 0026-3e08-1150
VLAN ID : 3
Sleep count : 3
Wireless mode : 802.11gn
Channel bandwidth : 20MHz
20/40 BSS Coexistence Management : Not supported
SM power save : Disabled
Short GI for 20MHz : Supported
Short GI for 40MHz : Supported
Short GI for 80MHz : Supported
Short GI for 160/80+80MHz : Not supported
STBC RX capability : Not supported
STBC TX capability : Not supported
LDPC RX capability : Not supported
SU beamformee capability : Not supported
MU beamformee capability : Not supported
Beamformee STS capability : N/A
Block Ack : TID 0 In
Supported VHT-MCS set : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set : 0, 1, 2, 3, 4, 5, 6, 7,
8, 9, 10, 11, 12, 13, 14,
15
Supported rates : 1, 2, 5.5, 6, 9, 11,
12, 18, 24, 36, 48, 54 Mbps
QoS mode : N/A
Listen interval : 10
RSSI : 62
Rx/Tx rate : 130/195 Mbps
Authentication method : Open system
Security mode : PRE-RSNA
AKM mode : Not configured
Cipher suite : N/A

User authentication mode : Bypass
WPA3 status : Disabled
Authorization CAR :
Average input rate : 102400 bps
Average output rate : 102400 bps
Authorization ACL ID : 3001(Not effective)
Authorization user profile : N/A
Roam status : N/A
Key derivation : SHA1
PMF status : Disabled
Forwarding policy name : Not configured
Online time : 0days 0hours 1minutes 13seconds
FT status : Inactive
BTM status : Disabled

表 1-5 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
IPv4 address	クライアントのIPv 4アドレス
IPv6 address	クライアントのIPv 6アドレス
Username	クライアントユーザ名。 クライアントのユーザ名（802.1X認証またはMAC認証を使用している場合） N/A（802.1X認証またはMAC認証を使用していない場合） メモ： クライアントがポータル認証を使用する場合、このフィールドにクライアントのポータルユーザ名は表示されません。
AID	アソシエーションID。
AP ID	クライアントが接続しているAPのID。
AP name	クライアントが接続しているAPの名前。
Radio ID	クライアントが接続している無線のID。
channel	クライアントが関連付けられている無線のチャネル。
SSID	クライアントが接続しているSSID。
VLAN ID	クライアントが属するVLAN ID
Sleep count	スリープ状態への遷移数。

フィールド	説明
Wireless mode	クライアントの動作モード: ● 802.11 a ● 802.11 b ● 802.11 g ● 802.11 gn ● 802.11 an ● 802.11 ac
Channel bandwidth	● チャネル帯域幅、20MHz、40MHz、80MHz、160MHz。
20/40 BSS Coexistence Management	クライアントが20 Mと40 Mの帯域幅の共存管理をサポートしているかどうか
SM Power Save	(未サポート)省電力モードの状態: ● Enabled:省電力モードを有効にすると、クライアントのアンテナのうち1つだけが動作状態になり、残りのアンテナはスリープ状態になります。 ● Disabled:省電力モードが無効になっています
Short GI for 20MHz	チャネル帯域幅が20MHzのときにクライアントがショートGIをサポートするかどうか。 Supported Not supported
Short GI for 40MHz	チャネル帯域幅が40MHzのときにクライアントがショートGIをサポートするかどうか。 Supported Not supported
Short GI for 80MHz	チャネル帯域幅が80MHzのときにクライアントがショートGIをサポートするかどうか。 Supported Not supported
Short GI for 160/80+80 MHz	チャネル帯域幅が160/80+80MHzのときにクライアントがショートGIをサポートするかどうか。 Supported. Not supported.
STBC Rx capability	クライアントSTBC受信能力 Not supported. Supported.
STBC Tx capability	クライアントSTBC送信能力 Not supported. Supported.
LDPC Rx capability	クライアントLDPC受信能力 Not supported. Supported.

フィールド	説明
SU beamformee capability	クライアントSU beamformee 能力 Not supported. Supported.
MU beamformee capability	クライアントMU beamformee 能力 Not supported. Supported.
Beamformee STS capability	クライアント beamformee STS能力 Not supported. Supported.。
Number of Sounding Dimensions	クライアントbeamformeeの空間ストリーム数: ● N/A ● 0~7
Block Ack	TIDを用いたブロックアックのネゴシエーション結果。 IN—受信方向からトラフィックのブロックアックを送信します。 OUT—送信方向からトラフィックのブロックアックを送信します。 BOTH—送受信方向からトラフィックのブロックアックを送信します。
Supported VHT-MCS set	クライアントによってサポートされたVHT-MCS
Supported HT MCS set	クライアントによってサポートされたHT-MCS
Supported rates	クライアントによってサポートされたレート
TWT scheduled	11axモードクライアントがスケジュール端末かどうか Yes:クライアントがTWTの端末をスケジュールします。 No:クライアントがTWT以外の端末をスケジュールする
QoS mode	QoS モード。 N/A—WMMに対応しません。 WMM—WMMに対応します。 WMM情報ネゴシエーションは、WMMをサポートするAPとクライアントの間で実行されます。
Listen interval	クライアントがビーコンフレームを受信するためにウェイクアップする間隔。 ビーコン間隔でカウントされます。
RSSI	受信した信号強度の表示。この値は、APによって検出されたクライアントの信号強度を示します。
Rx/Tx rate	データ、管理、制御フレームの送信および受信レート。
Speed	過去2分間の送受信レートの表示(Kbps単位)。小数点以下3桁で四捨五入。 N/A：送信レートと受信レートの両方が0の場合。

フィールド	説明
Authentication method	認証方式: ● Open system:オープンシステム認証 ● Shared key:共有鍵認証 ● SAE:SAE鍵認証
Security mode	セキュリティモード。 RSN—ビーコンおよびプローブ応答はRSN IEを伝送します。 WPA—ビーコンおよびプローブ応答はWPA IEを伝送します。 PRE-RSNA-ビーコンおよびプローブ応答はRSN IE/WPA IEを伝送しません。
AKM mode	AKMモード。 802.1X PSK Not configured.
Cipher suite	暗号スイート: ● N/A ● WEP40 ● WEP104 ● WEP128 ● CCMP ● TKIP ● GCMP
User authentication mode	ユーザ認証モード: Bypass MAC 802.1 X OUI
WPA3 status	WPA 3の状態: ● Disabled ● Enabled ● N/A:WPA 3セキュリティモードには対応していません。
Authorization CAR	● Average input rate :bps単位のアップストリーム平均レート ● Average output rate:bps単位のダウンストリーム平均レート

フィールド	説明
Authorization ACL ID	許可されたACL番号表示 ACL番号：許可されたACLが有効になった場合 ACL番号 + Not effective : 許可されたACLが無効になった場合 N/A：許可されたACLがない場合
Authorization user profile	許可されたユーザプロファイル名表示 許可されたユーザプロファイル名：許可されたACLが有効になった場合 許可されたユーザプロファイル名 + Not effective：許可されたACLが無効になった場合 N/A：許可されたユーザプロファイルがない場合
Roam status	Roam状態:: ● Roaming in progress ● Intra-AC roam ● N/A:クライアントは正常にオンラインになりました
Key derivation	キー派生タイプ： SHA1—HMAC-SHA1ハッシュアルゴリズムを使用します。 SHA256—HMAC-SHA256ハッシュアルゴリズムを使用します。 N/A—アルゴリズムを使用しません。
PMF status	PMF状態 Enabled—管理フレーム保護が有効になっています。 Disabled—管理フレーム保護が無効になっています。 N/A—管理フレームの保護は行われません。
Forwarding policy name	WLAN転送ポリシ Not configured— WLAN転送ポリシが設定されていません。 policy-name.
Online time	クライアントのオンライン期間。
FT status	Fast BSS transition (FT). ● Active:有効 ● Inactive:無効
BTM status	BSS transition management (BTM) Active-BTM有効 Inactive-BTM無効
Authorization user gruoup	認可されたユーザグループ

1.1.17 display wlan client failure

Syntax

display wlan client failure

View

すべての view

定義済みユーザロール

network-admin

説明

display wlan client failure コマンドはクライアントの接続失敗情報を表示します。

デバイスは、最大 512 の接続失敗情報を保存できます。失敗情報がこの上限を超えると、最も古いレコードが自動的に削除されます。

例

#クライアントの接続失敗情報を表示します。

<Sysname>display wlan client failure

```
Total association failures: 0
Total authentication failures: 0
-----------
Association failures:
 Client-info                      AP name    R SSID    Time

 Authentication failures:
 Client-info                      AP name    R SSID    Time
 8AE6-6CBB-AF91/-(-)                1451-7e0f- 3 anchor-1 2021-06-09 12:17:26
                                  50c0       x-nec
```

表 1-6 コマンド出力

フィールド	説明
Client-info	失敗したクライアントの情報です。MACアドレス、IPアドレス、ユーザ名が表示されます。情報がない部分は"-"で表示されます。
AP name	失敗したAP名
R	失敗したラジオのID
SSID	失敗したSSID
Time	失敗した時刻

1.1.18 display wlan client status

Syntax

display wlan client status [**mac-address** *mac-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H の形式で指定します。このオプションを指定しないと、すべてのクライアントに関するステータス情報が表示されます。

verbose: 詳細なクライアントのステータス情報を表示します。このキーワードを指定しない場合、コマンドはクライアント状況情報の概要を表示します。

説明

display wlan client status コマンドはクライアントステータス情報を表示します。

例

#指定されたクライアントの簡単なステータス情報を表示します

<Sysname> display wlan client status mac-address 001c-f08f-f804

```
Total number of clients: 1
MAC address     RSSI  Rx/Tx rate(bps)   Speed(bps)   Discard  AP name         RID
001c-f08f-f804  0     39/117Mbps        N/A          0.00%    ap2            2
```

#すべてのクライアントの簡単なステータス情報を表示します。

<Sysname> display wlan client status

```
Total number of clients: 2
MAC address     RSSI  Rx/Tx rate(bps)   Speed(bps)   Discard  AP name         RID
000b-c002-9d09  65    39/117Mbps        N/A          0.00%    ap2            2
000f-e265-6401  62    130/195Mbps       N/A 0.00%    ap1            1
```

表 1-7 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
access time	クライアントがWLANとの接続に要した時間
RSSI	クライアントのRSSI
Rx/Tx rate	クライアントがデータ、管理パケット、制御パケットを送受信する速度
Speed	過去2分間の送受信レートの表示(Kbps単位)。小数点以下3桁で四捨五入。 N/A：送信レートと受信レートの両方が0の場合。
Discard	クライアントに廃棄されるパケットの割合
AP name	クライアントが紐付いたAPの名前

フィールド	説明
RID	クライアントが紐付いた無線のID

#指定したクライアントの詳細なステータス情報を表示します。

<Sysname> display wlan client status mac-address 001c-f08f-f804 verbose

```
Total number of clients: 1
MAC address                    : 001c-f08f-f804
AP name                        : ap2
Radio ID                       : 2
RSSI                           : 0
Rx/Tx rate                     : 39/117 Mbps
Speed                          : N/A
Received:
 Retransmitted packets           : 84
 Retransmitted packet ratio      : 64.12 %
Sent:
 Retransmitted packets           : 0
 Retransmitted packet ratio      : 0.00 %
Discarded:
 Discarded packets               : 0
 Discarded packet ratio          : 0.00 %
```

表 1-8 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
AP name	クライアントの関連AP名
Radio ID	クライアントの関連付けRadio ID
RSSI	クライアントのRSSI
Rx/Tx rate	クライアントがパケットを送受信する速度(データ、管理、制御パケット)
Speed	過去2分間の送受信レートの表示(Kbps単位)。小数点以下3桁で四捨五入。 N/A：送信レートと受信レートの両方が0の場合。
Received	受信パケット統計情報 ● 再伝送パケット ● 再伝送パケット比率
Sent	送信パケット統計情報 ● 再伝送パケット ● 再伝送パケット比率
Discarded	廃棄パケット統計情報

フィールド	説明
	• 廃棄パケット • 廃棄パケット比率

関連コマンド

- wlan forwarding-policy

1.1.19 display wlan service-template

Syntax

display wlan service-template [*service-template-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。この引数を指定しない場合は、すべてのサービステンプレートに関する情報が表示されます。

verbose: 詳細なサービステンプレート情報を表示します。

説明

display wlan service-template コマンドはサービステンプレート情報を表示します。

例

すべてのサービステンプレートに関する簡易情報を表示します。

[Sysname] display wlan service-template

```
Total number of service templates: 2
Service template name          SSID                              Status
1                            2333                              Enabled
2                            3222                              Enabled
```

すべてのサービステンプレートに関する詳細情報を表示します。

<Sysname> display wlan service-template verbose

```
Service template name       : service1
Description                 : Not configured
```

```
SSID                      : wuxianfuwu
SSID-hide                 : Disabled
User-isolation            : Disabled
Service template status     : Disabled
Maximum clients per BSS     : 64
Frame format              : Dot3
Seamless roam status        : Disabled
Seamless roam RSSI threshold : 50
Seamless roam RSSI gap      : 20
VLAN ID                   : 1
AKM mode                  : PSK
Security IE               : RSN
Cipher suite              : CCMP
WEP key ID                : 1
TKIP countermeasure time    : 100 sec
PTK lifetime              : 43200 sec
PTK rekey                 : Enabled
GTK rekey                 : Enabled
GTK rekey method           : Time-based
GTK rekey time            : 86400 sec
GTK rekey client-offline    : Enabled
WPA3 status               : Disabled
PPSK                      : Disabled
PPSK Fail Permit           : Enabled
User authentication mode    : Bypass
Intrusion protection        : Disabled
Intrusion protection mode   : Temporary-block
Temporary block time        : 180 sec
Temporary service stop time  : 20 sec
Fail VLAN ID              : 1
802.1X handshake           : Enabled
802.1X handshake secure     : Disabled
802.1X domain             : my-domain
MAC-auth domain           : Not configured
Max 802.1X users per BSS    : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate      : Enabled
Authorization fail mode     : Online
Accounting fail mode        : Online
Authorization             : Permitted
Key derivation            : SHA1
PMF status                : Optional
Hotspot policy number       : Not configured
```

```
Forwarding policy status    : Disabled
Forwarding policy name      : Not configured
Forwarder                 : AP
FT status                 : Disabled
QoS trust                 : Port
QoS priority              : 0
BTM status                : Disabled
```

表 1-9 コマンド出力

フィールド	説明
SSID	サービステンプレートのSSID
SSID-hide	SSID非表示: ● Disabled:SSIDアドバタイズメントの有効化 ● Enabled:SSIDアドバタイズメントを無効にする
User-isolation	ユーザアイソレーション: ● Disabled ● Enabled
Service template status	サービステンプレートの状態: ● Disabled ● Enabled
Maximum clients per BSS	BSSがサポートするクライアントの最大数。
Frame format	クライアントデータパケットのカプセル化形式: ● Dot 3:802.3 ● Dot11:802.11
Seamless roam status	このフィールドは、現在のソフトウェアバージョンではサポートされていません。 シームレスなローミングの状態: ● Disable ● Enable
Seamless roam RSSI threshold	このフィールドは、現在のソフトウェアバージョンではサポートされていません。 シームレスローミングRSSIしきい値。
Seamless roam RSSI gap	このフィールドは、現在のソフトウェアバージョンではサポートされていません。 シームレスなローミングRSSIギャップ。
VLAN ID	クライアントが指定されたサービステンプレートからオンラインになった後に属するVLAN
AKM mode	AKMモード: ● 802.1 X ● PSK

フィールド	説明
Security IE	セキュリティIEの種類: ● RSN ● WPA
Cipher suite	暗号化スイート: ● WEP40 ● WEP104 ● WEP128 ● TKIP ● CCMP ● GCMP
TKIP countermeasure time	TKIP対策時間。 設定値0は、対策が取られていないことを表します。
PTK life time	PTKの生存期間
PTK rekey	PTK更新機能ステータス: ● Enabled ● Disabled
GTK rekey	GTK rekeyが有効/無効 : ● Enabled ● Disabled
GTK rekey method	GTKの更新方法: ● Time-based:時間ベースの更新 ● Packet-based:パケット数に基づく更新
GTK rekey time	GTK rekey間隔.
GTK rekey packets	GTKをリフレッシュする前に送信できるパケット数。
GTK rekey client-offline	クライアントオフライン更新機能ステータス: ● Enabled ● Disabled
WPA3 status	WPA 3セーフモードの状態: ● Disabled ● Mandatory ● Optional
PPSK	PPSK機能ステータス: ● Disabled ● Enabled
PPSK Fail Permit	PPSKワイヤレスユーザ脱出機能の状態: ● Disabled Enabled

フィールド	説明
User authentication mode	認証モードには、次のものがあります。 ● Bypass: ● MAC ● 802.1 X ● MAC-and-802.1X
Intrusion protection	● client-off GTK rekeyが有効/無効： ● Enabled ● Disabled
Intrusion protection mode	侵入防止モード： Temporary-block－ブロックリストに侵入者を一時的に追加します。 Service-stop－リセットされるまで、不正なパケットを受信するBSSによって提供されるすべてのサービスを停止します。 Temporary-service-stop－不正なパケットを受信したBSSが提供するアクセスサービスを一時的に停止します。
Temporary block time	一時的なブロック時間（秒）。
Temporary service stop time	一時的なサービス停止時間（秒）。
Fail VLAN ID	認証サーバが正常で認証に合格できない場合に、クライアントが追加されるVLANのID。未設定の場合“Not configured”が表示されます。
Critical VLAN ID	認証サーバに到達できないために認証を渡すことができない場合に、クライアントが追加されるVLANのID。クリティカルVLAN IDが設定されていない場合、このフィールドにはNot configuredと表示されます。
802.1 X handshake	802.1Xハンドシェイクが有効/無効： Enabled. Disabled.
802.1 X handshake secure	802.1 Xセキュアハンドシェイクが有効/無効： ● Enabled ● Disabled
802.1 X domain	802.1X認証ドメイン。未設定の場合“Not configured”が表示されます。
MAC-auth domain	MAC認証ドメイン。未設定の場合“Not configured”が表示されます。
Max 802.1X users per BSS	BSSでサポートされている802.1Xユーザの最大数
Max MAC-auth users per BSS	BSSでMAC認証に合格するサポートされるユーザの最大数。

フィールド	説明
Authorization fail mode	許可失敗モード Offline－認証に失敗すると、クライアントはログオフされます。 Online－認証に失敗しても、クライアントはログオフされません。
Accounting fail mode	アカウンティング失敗モード Offline－アカウンティングに失敗すると、クライアントはログオフされます。 Online－アカウンティングに失敗しても、クライアントはログオフされません。
Authorization	許可情報： Permitted－RADIUSサーバまたはローカルデバイスによって発行された許可情報を適用します。 Ignored－RADIUSサーバまたはローカルデバイスによって発行された認証情報を無視します。
Key derivation	キーの導出タイプ ● SHA1－HMAC-SHA1 hash algorithm使用 ● SHA256－HMAC-SHA256 hash algorithm使用 ● SHA1-AND-SHA256－HMAC SHA1 and SHA256 hash algorithm使用
PMF status	PMF状態 ● Disabled－管理フレームの保護が無効になっています。 ● Optional－オプションモードでの管理フレーム保護が有効になっています。 ● Mandatory－必須モードの管理フレーム保護が有効になっています。
Hotspot policy number	このフィールドは、現在のソフトウェアバージョンではサポートされていません。 ホットスポット2.0ポリシー番号。
Forwarding policy status	転送ポリシーの状態: ● Disabled ● Enabled
Forward policy name	転送ポリシー名: ● Not configured ● policy-name
Forwarder	クライアントデータパケットの転送先: ● AC ● AP

フィールド	説明
FT status	FT状態 ● Disabled ● Enabled
FT method	クイックBSS切り替え ● over-the-air
FT reassociation deadline	再関連付けのタイムアウト時間 (秒)
QoS trust	QoSトラステッドモード: ● Port ● Dot11e
QoS priority	ポートプライオリティ:0~7の範囲
BTM status	BTM機能状態: Disabled Enabled

1.1.20 display wlan statistics client

Syntax

display wlan statistics client [**mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address* : 指定された MAC アドレスのクライアント統計を表示します。このパラメータが指定されていない場合、すべてのクライアント統計が表示されます。

説明

display wlan statistics client コマンドを使用して、クライアントの統計情報を表示します。

例

すべてのワイヤレス クライアントの統計を表示します。

<Sysname> display wlan statistics client

```
MAC address              : 0014-6c8a-43ff
```

```
AP name                 : ap1
Radio ID                : 1
SSID                    : office
BSSID                   : 000f-e2ff-7700
RSSI                    : 31
Sent frames :
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 9/1230 (frames/bytes)
  Video                 : 0/0 (frames/bytes)
  Voice                 : 2/76 (frames/bytes)
Received frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 18/2437 (frames/bytes)
  Video                 : 0/0 (frames/bytes)
  Voice                 : 7/468 (frames/bytes)
Discarded frames :
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 0/0 (frames/bytes)
  Video                 : 0/0 (frames/bytes)
  Voice                 : 5/389 (frames/bytes)
```

表 1-10 コマンド出力

フィールド	説明
SSID	クライアントに関連付けられたSSID
MAC address	クライアントのMACアドレス
RSSI	APがClientの信号強度を検出したことを示す受信信号強度インジケータ
Sent frames	送信フレーム数
Back ground	AC-BKキュー。
Best effort	AC-BEキュー。
Video	AC-VIキュー。
Voice	AC-VOキュー。
Received frames	受信フレーム数
Discarded frames	廃棄パケット数

1.1.21 display wlan statistics connect-history

Syntax

display wlan statistics connect-history service-template *service-template-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template *service-template-name* : サービステンプレートのクライアント接続履歴情報を表示します。

説明

display wlan statistics connect-history コマンドはクライアント接続履歴情報を表示します。

例

#サービステンプレート 1 の AP のクライアント接続履歴情報を表示します。

<Sysname> display wlan statistics connect-history service-template 1

```
AP name                  : ap1
Radio ID                 : 1
Associations              : 132
Association failures       : 3
Reassociations            : 30
Rejections               : 12
Abnormal disassociations    : 2
Current associations       : 57
```

1.1.22 display wlan statistics service-template

Syntax

display wlan statistics service-template *service-template-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template-name : 指定されたサービステンプレートに関する統計を表示します。

説明

display wlan statistics service-template コマンドを使用して、サービステンプレートの統計情報を表示します。

例

#サービステンプレート 1 の統計情報を表示します。

<Sysname> display wlan statistics service-template 1

```
AP name                    : ap1
Radio ID                   : 1
Received :
  Frame count              : 1713
  Frame bytes              : 487061
  Data frame count         : 1683
  Data frame bytes         : 485761
  Association request count  : 2
Sent :
  Frame count              : 62113
  Frame bytes              : 25142076
  Data frame count         : 55978
  Data frame bytes         : 22626600
  Association response count  : 2
```

表 1-11 コマンド出力

フィールド	説明
AP name	AP名
Radio ID	無線ID番号
Received	受信統計: • Frame count:受信フレーム数 • Frame bytes:受信フレームバイト数 • Data frame count:受信データフレーム数 • Data frame bytes:受信データフレームのバイト数 • Association request count:受信接続要求フレーム数
Sent	送信統計: • Frame count:フレーム数の送信 • Frame bytes:送信フレームバイト数 • Data frame count:送信データフレーム数 • Data frame bytes:送信データフレームのバイト数 • Association response count:接続応答フレーム数の送信

関連コマンド

- wlan vip-client-group
- client-mac

1.1.23 display wlan whitelist

Syntax

display wlan whitelist

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan whitelist コマンドを使用して、ホワイトリストを表示します。

例

#ホワイトリストを表示する。

<Sysname> display wlan whitelist

```
Total number of clients: 3
 MAC addresses:
  000e-35b2-000e
  0019-5b8e-b709
  001c-f0bf-9c92
```

1.1.24 nas-id

Syntax

nas-id *nas-id*

undo nas-id

デフォルト

設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

nas-id : NAS ID を指定します。 NAS ID は、 1～63 文字の文字列です。大文字と小文字を区別します。

説明

nas-id コマンド は ネットワークアクセスサーバ識別子（ NAS ID ）を設定します。

オンラインになると、クライアントは RADIUS 要求を送信し、NAS ID を RADIUS サーバに送信してネットワークアクセスサーバを示します。

AP view、AP group view、および Global configuration view の設定の優先順位は降順です。NAS ID は、サービステンプレートを無線にバインドするときにも設定できます。サービステンプレートを無線にバインドするときに NAS ID を指定した場合、AP はサービステンプレートに指定された NAS ID を使用します。

NAS-IN は、次の方法で指定できます。

1. サービステンプレートを無線にバインドする時に指定した NAS ID パラメータ
2. AP view の設定
3. AP group view の設定
4. wlan global configuration view の設定
5. ISP domain view の設定

NAS-ID 設定が存在しない場合、デバイスは **sysname** コマンドを使用して設定されたデバイス名を NAS-ID として使用します。

例

AP ap1 に abc123 を設定します。

<Sysname> system-view

[Sysname] wlan ap ap1 model WA6320

[Sysname-wlan-ap-ap1] nas-id abc123

AP group group1 に abc123 を設定します。

<Sysname> system-view

[Sysname] wlan ap-group group1

[Sysname-wlan-ap-group-group1] nas-id abc123

abc123 に abc123 を設定します。

<Sysname> system-view

[Sysname] wlan global-configuration

[Sysname-wlan-global-configuration] nas-id abc123

1.1.25 nas-port-id

Syntax

nas-port-id *nas-port-id*

undo nas-port-id

デフォルト

設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

nas-port-id : NAS port ID を指定します。 NAS port ID は、1～63 文字の文字列です。大文字と小文字を区別します。

説明

nas-port-id コマンド は ネットワークアクセスサーバのポート識別子（ NAS port ID を設定します。

undo nas-port-id コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートを無効にしてください。

オンラインになると、クライアントは RADIUS 要求を送信し、NAS port ID を RADIUS サーバに送信してネットワークアクセスサーバを示します。

AP view、AP group view、および Global configuration view の設定の優先順位は降順です。NAS port ID は、サービステンプレートを無線にバインドするときにも設定できます。サービステンプレートを無線にバインドするときに NAS port ID を指定した場合、AP はサービステンプレートに指定した NAS port ID を使用します。

例

NAS port ID を abcd1234 に設定します。

<Sysname> system-view

[Sysname] wlan ap ap1 model WA6320

[Sysname-wlan-ap-ap1] nas-port-id abcd1234

NAS port ID を abcd1234 に設定します。

<Sysname> system-view

[Sysname] wlan ap-group group1

[Sysname-wlan-ap-group-group1] nas-port-id abcd1234

global NAS port ID を abcd1234 に設定します。

<Sysname> system-view

[Sysname] wlan global-configuration

[Sysname-wlan-global-configuration] nas-port-id abcd1234

1.1.26 reset wlan client

Syntax

reset wlan client { **all** | **mac-address** *mac-address* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all:すべてのクライアントから切断します。

mac-address *mac-address*:指定したクライアントから切断します。

説明

reset wlan client コマンドはクライアントから切断します。

例

#すべてのクライアントから切断します。

<Sysname> reset wlan client all

関連コマンド

- display wlan client

1.1.27 reset wlan dynamic-blacklist

Syntax

reset wlan client { **all** | **mac-address** *mac-address* }

View

User view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: MAC アドレスでクライアントを指定します。このオプションを指定しないと、このコマンドはダイナミックブラックリストからすべてのクライアントを削除します。

説明

reset wlan dynamic-blacklist コマンドは指定したクライアントまたはすべてのクライアントをダイナミックブラックリストから削除します。

例

ダイナミックブラックリストからすべてのクライアントを削除します。

<AC> reset wlan dynamic-blacklist

ダイナミックブラックリストから指定したクライアントを削除します。

<AC> reset wlan dynamic-blacklist mac-address b8ca-32a2-df69

関連コマンド

- display wlan blacklist

1.1.28 reset wlan statistics client

Syntax

reset wlan statistics client { **all** | **mac-address** *mac-address* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべてのクライアントを指定します。

mac-address *mac-address*: クライアントを MAC アドレスで指定します。

説明

reset wlan statistics client コマンドはクライアントの統計情報を削除します。

例

すべてのクライアントの統計情報を削除します。

<AC> reset wlan statistics client all

関連コマンド

- display wlan statistics

1.1.29 reset wlan statistics service-template

Syntax

reset wlan statistics service-template *service-template-name*

View

User view

定義済みユーザロール

network-admin

パラメータ

service-template-name :サービステンプレート名で、1 ～ 63 文字の文字列です。大文字と小文字を区別しません。

説明

reset wlan statistics service-template コマンドを使用して、サービステンプレートの統計情報を削除します。

この機能を設定すると、サービステンプレートの統計情報を削除します。

例

#ワイヤレスサービステンプレート service1 の統計情報を削除します。

<Sysname> reset wlan statistics service-template service1

1.1.30 service-template

Syntax

service-template *service-template-name* [**vlan** *vlan-id*] [**ssid-hide**] [**nas-port-id** *nas-port-id*] [**nas-id** *nas-id*]

undo service-template *service-template-name*

デフォルト

radio view：AP group radio view の設定を使用します。

AP group radio view：設定なし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

vlan *vlan-id*: VLAN ID によって無線にバインドされる VLAN を指定します。範囲は 1～4094 です。このオプションを指定しない場合、無線はサービステンプレートにバインドされた VLAN を使用します。指定された VLAN が存在しない場合、このコマンドはクライアントがオンラインになったときに VLAN を作成します。

ssid-hide: ビーコンフレームで SSID を非表示にします。

nas-port-id *nas-port-id*: NAS port ID を指定します。NAS port ID は、1～63 文字のスペースを含まない文字列です。大文字と小文字を区別しません。

nas-id *nas-id*: NAS ID を指定します。NAS ID は、1～63 文字のスペースを含まない文字列です。大文字と小文字を区別しません。

説明

service-template コマンドはサービステンプレートを無線インタフェースまたは無線インタフェースにバインドします。

undo service-template コマンドは無線または無線インタフェースからサービステンプレートをバインド解除します。

サービステンプレートは、無線または無線インタフェースにバインドする前に作成する必要があります。

このコマンドを使用して設定された VLAN ID は、サービステンプレート用に設定された VLAN ID よりも優先されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

サービステンプレート service1 を radio 1 にバインドします。

<AC> system-view

[AC] wlan ap ap1

[AC-ap-ap1] radio 1

[AC-ap-ap1-radio-1] service-template service1

サービステンプレート service1 を Vlan10 を指定して AP group apgroup1 の radio 1 にバインドします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1240

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240-radio-1]service-template service1 vlan 2

1.1.31 service-template enable

Syntax

service-template enable

undo service-template enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

service-template enable コマンドはサービステンプレートを有効にします。

undo service-template enable コマンドはサービステンプレートを無効にします。

AC 上の BSS（basic service set）の数が制限を超える場合、新しいサービステンプレートを有効にできません。

例

サービステンプレート service1 を有効にします。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] service-template enable

1.1.32 snmp-agent trap enable wlan client

Syntax

snmp-agent trap enable wlan client

undo snmp-agent trap enable wlan client

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan client コマンドは WLAN アクセスの SNMP 通知を有効にします。

undo snmp-agent trap enable wlan client コマンドはデフォルトに戻します。

この機能を有効にすると、クライアントのステータスが変更されるたびに、装置は NMS にクライアントステータス変更通知を送信します。

例

#WLAN アクセスに対して SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan client

1.1.33 ssid

Syntax

ssid *ssid-name*

undo ssid

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ssid-name:サービステンプレートの SSID を、大文字と小文字を区別して 1~32 文字の文字列で指定します。

説明

ssid コマンドはサービステンプレートの SSID を設定します。

undo ssid コマンドはサービステンプレートの SSID を削除します。

このコマンドを実行する前に、サービステンプレートを無効にしてください。

例

サービステンプレート service1 に SSID lynn を設定します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] ssid lynn

1.1.34 unknown-client

Syntax

unknown-client { **deauthenticate** | **drop** }

undo unknown-client

デフォルト

AP は未知のクライアントからのパケットを廃棄し、未知のクライアントの認証を解除します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

deauthenticate: 不明なクライアントからのパケットを廃棄し、これらのクライアントの認証を解除します。

drop: 不明なクライアントからのパケットを廃棄します。

説明

unknown-client コマンドは AP が未知のクライアントからのトラフィックを処理する方法を設定します。

undo unknown-client コマンドはデフォルトに戻します。

例

AP ap1 サービステンプレート example に未知のクライアントからのパケットを廃棄するが、未知のクライアントの認証は解除しない設定をします。

<AC> system-view

[AC] wlan service-template example

[AC -wlan-st-example] unknown-client drop

1.1.35 vlan

Syntax

vlan *vlan-id*

undo vlan

デフォルト

サービステンプレートを使用してオンラインになった後、クライアントは VLAN 1 に割り当てられます。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN を VLAN ID で指定します。VLAN ID の設定範囲は 1～4094 です。指定した VLAN が存在しない場合、このコマンドは、クライアントがオンラインになったときに VLAN を作成します

説明

vlan コマンドはサービステンプレートを使用してオンラインになっているクライアントを VLAN に割り当てます。

undo vlan コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートを無効にしてください。

指定した VLAN が存在しない場合、このコマンドはクライアントがオンラインになったときに VLAN を作成します。

例

サービステンプレート service1 を介してオンラインになっているクライアントを VLAN 2 に割り当てます。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1] vlan 2

1.1.36 wlan client failure history aging

Syntax

wlan client failure history aging *aging-time*

undo wlan client failure history aging

デフォルト

72 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time:クライアントオンボード障害レコードのエージングタイマを 1 時間から 720 時間の範囲で指定します。

説明

クライアントオンボード障害レコードのエージングタイマを指定するには **wlan client failure history aging** コマンドを使用します。

デフォルトに戻すには、**undo wlan client failure history aging** コマンドを使用します。

デバイスは、最大 512 のクライアントオンボード障害レコードを保存できます。レコード数がこの上限を超えると、最も古いレコードが自動的に削除されます。レコード数がこの上限を超えていなくても、このコマンドで指定したエージングタイマがタイムアウトした場合は、すべてのレコードが削除されます。

例

クライアントオンボード障害レコードのエージングタイマを 700 時間に設定します。

<Sysname> system-view

[Sysname] wlan client failure history aging 700

1.1.37 wlan client reauthentication-period

Syntax

wlan client reauthentication-period [*period-value*]

undo wlan client reauthentication-period

デフォルト

10 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

period-value : アイドル期間。値の範囲は 1 ～ 3600 秒です。

説明

wlan client reauthentication-period コマンドを使用して、クライアントの再認証の前にアイドル期間を設定します。

undo wlan client reauthentication-period コマンドはデフォルトに戻します。

クライアントが再認証を行い、VLAN を切り替えるネットワーク環境では、クライアントの再認証前のアイドル期間を設定することをお勧めします。

アイドル期間が設定されると、デバイスは認証されたクライアントの MAC アドレスをダイナミックブラックリストに追加し、指定された期間内のクライアントのアクセスを禁止します。この方法でダイナミックブラックリストに追加された MAC アドレスは、ダイナミックブラックリストのエージングタイムの影響を受けません。

例

クライアント再認証の前にアイドル期間を 100 秒に設定します。

<Sysname> system-view

[Sysname] wlan client reauthentication-period 100

1.1.38 wlan dynamic-blacklist active-on-ap

Syntax

wlan dynamic-blacklist active-on-ap

undo wlan dynamic-blacklist active-on-ap

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan dynamic-blacklist active-on-ap コマンドはダイナミックブラックリストを AP で有効にするように設定します。

undo wlan dynamic-blacklist active-on-ap コマンドはダイナミックブラックリストを AC に適用するように設定します。

ダイナミックブラックリストを AC に適用するように設定すると、AC に接続されているすべての AP はダイナミックブラックリストのクライアントを拒否します。ダイナミックブラックリストを AP に適用するように設定すると、ダイナミックブラックリスト内のクライアントに関連付けられている AP はクライアントを拒否しますが、クライアントは引き続き AC に接続されている他の AP と関連付けることができます。ダイナミックブラックリストを高密度環境で AC に適用するように設定することを推奨します。

例

ダイナミックブラックリストを AC 上で有効にするように設定します。

<AC> system-view

[AC] undo wlan dynamic-blacklist active-on-ap

1.1.39 wlan dynamic-blacklist lifetime

Syntax

lan dynamic-blacklist lifetime *lifetime*

undo wlan dynamic-blacklist lifetime

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

lifetime: エージング時間を指定します。設定範囲は 1～3600 秒です。

説明

wlan dynamic-blacklist lifetime コマンドはダイナミックブラックリストエントリのエージングタイムを設定します。

undo wlan dynamic-blacklist lifetime コマンドはデフォルトに戻します。

設定したエージング時間は、設定後、ダイナミックブラックリストに追加されたエントリから有効です。

例

#ダイナミックブラックリストのエージング時間を 3600 秒に指定します。

<AC> system-view

[AC] wlan dynamic-blacklist lifetime 3600

1.1.40 wlan link-test

Syntax

wlan link-test *mac-address*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

mac-address: H-H-H 形式でクライアント MAC アドレスを指定します。

説明

wlan link-test コマンドはワイヤレスリンクの品質をテストします。

無線リンク品質検出により、AP は無線クライアントへのリンクの品質をテストできます。AP は、各サポートレートでクライアントに空のデータフレームを送信します。次に、クライアントからの応答に基づいて、RSSI、パケット再送信、RTT などのリンク品質情報を計算します。

無線リンク品質検出のタイムアウト時間は 10 秒です。タイムアウト時間内で無線リンク検出が完了しない場合、テスト結果を取得できません。

例

MAC アドレス 60a4-4cda-eff0 のクライアントに対して、無線リンク品質検出を実行します。

<AC> wlan link-test 60a4-4cda-eff0

<Sysname> wlan link-test 60a4-4cda-eff0

```
Testing link to 60a4-4cda-eff0. Press CTRL + C to break.
                        Link Status
--------------------------------------------------------------------------
MAC address: 60a4-4cda-eff0
--------------------------------------------------------------------------
VHT-MCS  Rate(Mbps)  Tx packets  Rx packets  RSSI   Retries RTT(ms)
--------------------------------------------------------------------------
NSS = 1
--------------------------------------------------------------------------
 0      32.5        5           5           54     0       0
 1      65          5           5           51     0       0
 2      97.5        5           5           49     0       0
 3      130         5           5           47     0       0
 4      195         5           5           45     0       0
```

```
 5      260        5          5          45     0       0
 6      292.5      5          5          44     0       0
 7      325        5          5          44     0       0
 8      390        5          5          44     0       0
 9      433.3      5          5          43     0       0
------------------------------------------------------------------------
NSS = 2
------------------------------------------------------------------------
0      65         5          5          44     0       0
1      130        5          5          44     0       0
2      195        5          5          44     0       0
3      260        5          5          44     0       0
 4      390        5          5          44     0       0
 5      520        5          5          44     0       0
 6      585        5          5          43     0       0
 7      650        5          5          43     0       0
 8      780        5          5          43     0       0
 9      866.7      5          5          43     0       0
```

#MAC アドレスが 60 a4-4cda-eff0 のクライアントを無線リンク品質検出を実行します。

<Sysname> wlan link-test 784f-43b6-077c

```
Testing link to 784f-43b6-077c. Press CTRL + C to break.
                          Link Status
------------------------------------------------------------------------
MAC address: 784f-43b6-077c
------------------------------------------------------------------------
MCS    Rate(Mbps)  Tx packets  Rx packets  RSSI   Retries  RTT(ms)
------------------------------------------------------------------------
0      6.5        5          5          54     0       0
1      13         5          5          51     0       0
2      19.5       5          5          49     0       0
3      26         5          5          47     0       0
4      39         5          5          45     0       0
5      52         5          5          45     0       0
6      58.5       5          5          44     0       0
7      72.2       5          5          44     0       0
8      13         5          5          44     0       0
9      26         5          5          43     0       0
10      39        5          5          44     0       0
11      52        5          5          44     0       0
12      78        5          5          44     0       0
13      104       5          5          44     0       0
14      117       5          5          44     0       0
```

```
15      144.4     5         5         44    11      0
```

表 1-12 コマンド出力

フィールド	説明
No./MCS/VHT-MCS	• No－802.11a、802.11b、802.11gクライアントのリンク品質テストの速度番号。 • MCS－802.11nクライアントのリンク品質テストのMCSインデックス。 • VHT-MCS－802.11acクライアントのリンク品質テストのVHT-MCSインデックス。
Rate (Mbps)	APが無線リンク品質検出パケットを送信するレート
Tx packets	APが送信する無線リンク品質検出パケットの個数
Rx packets	APが受信したクライアント応答メッセージの数
RSSI	APがクライアントの信号強度を検出したことを示す受信信号強度インジケータ
Retries	APが無線リンク品質検出パケットを再送信した回数
RTT (ms)	APが無線リンク品質検出パケットを送信してからクライアント応答を受信するまでの平均ラウンドトリップ時間
NSS	802.11nまたは802.11acクライアントのリンク品質チェックのための空間ストリーム数

1.1.41 wlan nas-port-id format

Syntax

wlan nas-port-id format { **2** | **4** }

undo wlan nas-port-id format

デフォルト

2

View

System view

定義済みユーザロール

network-admin

パラメータ

2:フォーマット 2（SlotID00IfNOVlanID）を指定します。このフォーマットにおいて、NAS ポート ID は以下の情報を含みます。

- SlotID－クライアントがアクセスするスロットの 2 桁の ID です。

- IfNOークライアントがアクセスするインタフェースの 3 桁の番号です。
- VlanIDークライアント VLAN の 9 桁の ID です。

4: フォーマット 4（slot=**;subslot=**;port=**;vlanid=**;vlanid2=**）を指定します。vlanid2=**は、VLAN ターミネーションが有効なインタフェースで WLAN にアクセスするクライアントに対してのみ使用します。

説明

wlan nas-port-id format コマンドは NAS port ID フォーマットを指定します。

undo wlan nas-port-id format コマンドはデフォルトに戻します。

802.1 X および MAC 認証クライアントは、指定された形式の NAS ポート ID を RADIUS パケットで提供します。

nas-port-id コマンドを使用して NAS ポート ID が指定されている場合、クライアントは指定された NAS ポート ID を使用します。

例

NAS port ID フォーマットにフォーマット 4 を指定します。

<AC> system-view

[AC] wlan nas-port-id format 4

1.1.42 wlan permit-ssid

Syntax

wlan permit-ssid *ssid-name*

undo wlan permit-ssid [*ssid-name*]

デフォルト

設定なし

View

User profile view

定義済みユーザロール

network-admin

パラメータ

ssid-name:名前で SSID を指定します。1 文字以上 32 文字以下で、大文字と小文字が区別されます。

説明

wlan permit-ssid コマンドはクライアントアソシエーションの許可された SSID を指定します。

undo permit-ssid コマンドは許可された SSID を削除します。

クライアントアソシエーションに許可された SSID が指定されていない場合、クライアントアソシエーションは制限されません。

クライアントアソシエーションに許可された SSID を指定した場合、クライアントは SSID を介してのみ WLAN と関連付けることができます。

ssid-name 引数を指定しない場合、コマンドの **undo** 形式は許可されたすべての SSID を削除します。

例

クライアントアクセスの許可される SSID として、SSID ssid1 を指定します。

<Sysname> system-view

[Sysname] user-profile profile1

[Sysname-user-profile- profile1] wlan permit-ssid ssid1

1.1.43 wlan service-template

Syntax

wlan service-template *service-template-name*

undo wlan service-template *service-template-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

mdc-admin

パラメータ

service-template-name：ワイヤレスサービステンプレートの名前で、1 ～ 63 文字の文字列です。大文字と小文字を区別しません。

説明

wlan service-template コマンドを使用してサービステンプレートを作成し、ワイヤレス Service template view に入ります。

undo wlan service-template コマンドを使用して、サービステンプレートを削除します。

サービス テンプレートを削除するときに、サービステンプレートが無線にマッピングされている場合、そのサービステンプレートは、マッピングが解除されるまで削除できません。

例

サービステンプレート service1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan service-template service1

[AC-wlan-st-service1]

1.1.44 wlan static-blacklist mac-address

Syntax

wlan static-blacklist mac-address *mac-address*

undo wlan static-blacklist [**mac-address** *mac-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H の形式で指定します。

説明

wlan static-blacklist mac-address コマンドはスタティックブラックリストにクライアントを追加します。

undo wlan static-blacklist mac-address コマンドはスタティックブラックリストからクライアントを削除します。

スタティックブラックリストにオンラインクライアントを追加すると、クライアントをログオフします。

ホワイトリストとスタティックブラックリストの両方にクライアントを追加することはできません。

undo コマンドで、**mac-address** *mac-address* オプションを省略した場合、スタティックブラックリストからすべてのクライアントを削除します。

例

スタティックブラックリストに MAC アドレス 001c-f0bf-9c92 を追加します。

<AC> system-view

[AC] wlan static-blacklist mac-address 001c-f0bf-9c92

関連コマンド

- display wlan blacklist

1.1.45 wlan whitelist mac-address

Syntax

wlan whitelist mac-address *mac-address*

undo wlan whitelist [**mac-address** *mac-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H の形式で指定します。

説明

wlan whitelist mac-address コマンドはホワイトリストにクライアントを追加します。

undo wlan whitelist mac-address コマンドはホワイトリストからクライアントを削除します。

最初のクライアントをホワイトリストに追加すると、すべてのオンラインクライアントを切断するかどうかを尋ねるメッセージが表示されます。“Y”と入力するとホワイトリストが作成されます。

ホワイトリストからオンラインクライアントを削除すると、クライアントをログオフします。ホワイトリストからすべてのクライアントを削除すると、オンラインクライアントはログオフされません。

ホワイトリストとスタティックブラックリストの両方にクライアントを追加することはできません。

undo コマンドで、**mac-address mac-address** オプションを省略した場合、ホワイトリストからすべてのクライアントを削除します。

例

ホワイトリストに MAC アドレス 001c-f0bf-9c92 を追加します。

<Sysname> system-view

[Sysname] wlan whitelist mac-address 001c-f0bf-9c92

```
This command will disconnect all clients.Continue?[Y/N]:
```

関連コマンド

- display wlan whiteliest

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

7.AP 管理

本マニュアルは以下に示す章で構成されています。

01-AP 管理
02-コンフィグレーションプロファイルの設定

目次

このセクションのページは **7-x-x** です。

1 章 AP 管理 1-1
1.1 AP 管理設定コマンド 1-1
1.1.1 ap 1-1
1.1.2 ap-model 1-2
1.1.3 bridge-aggregation 1-2
1.1.4 data-tunnel encryption 1-4
1.1.5 delete file 1-5
1.1.6 description 1-6
1.1.7 description 1-7
1.1.8 display wlan ap 1-7
1.1.9 display wlan ap address 1-25
1.1.10 display wlan ap all feature capwap 1-26
1.1.11 display wlan ap connection-record 1-28
1.1.12 display wlan ap diagnostic-information 1-29
1.1.13 display wlan ap files 1-29
1.1.14 display wlan ap online-time 1-30
1.1.15 display wlan ap reboot-log 1-31
1.1.16 display wlan ap region-code 1-33
1.1.17 display wlan ap running-configuration 1-34
1.1.18 display wlan ap statistics association-failure-record 1-36
1.1.19 display wlan ap statistics cloud-cluster switch-over-state 1-38
1.1.20 display wlan ap statistics image-download 1-42
1.1.21 display wlan ap statistics online-record 1-45
1.1.22 display wlan ap-group 1-47
1.1.23 display wlan ap-model 1-49
1.1.24 download file 1-51
1.1.25 echo-count 1-51
1.1.26 echo-interval 1-52
1.1.27 firmware-upgrade 1-54
1.1.28 fragment-size 1-55
1.1.29 gigabitethernet 1-56
1.1.30 hybrid-remote-ap 1-57
1.1.31 if-match ip 1-58
1.1.32 keepalive-interval 1-59
1.1.33 led-mode 1-60
1.1.34 mac-address 1-61

1.1.35 mac-address 1-62
1.1.36 map-configuration 1-63
1.1.37 port-isolate enable 1-64
1.1.38 port access vlan 1-66
1.1.39 port hybrid pvid 1-67
1.1.40 port hybrid vlan 1-69
1.1.41 port link-aggregation group 1-71
1.1.42 port link-type 1-73
1.1.43 port trunk permit vlan 1-74
1.1.44 port trunk pvid 1-76
1.1.45 power-level default 1-78
1.1.46 priority 1-80
1.1.47 region-code 1-81
1.1.48 region-code-lock 1-82
1.1.49 remote-configuration 1-83
1.1.50 remote-configuration synchronize 1-85
1.1.51 reset wlan ap 1-86
1.1.52 reset wlan ap connection-record 1-87
1.1.53 reset wlan ap reboot-log 1-87
1.1.54 reset wlan ap statistics association-failure-record 1-88
1.1.55 reset wlan ap statistics image-download 1-89
1.1.56 reset wlan ap statistics online-record 1-90
1.1.57 reset wlan ap statistics tunnel-down-record 1-90
1.1.58 reset wlan ap statistics switch-over-record 1-91
1.1.59 retransmit-count 1-91
1.1.60 retransmit-interval 1-93
1.1.61 serial-id 1-94
1.1.62 serial-id 1-95
1.1.63 smartrate-ethernet 1-96
1.1.64 snmp-agent trap enable wlan ap 1-97
1.1.65 snmp-agent trap enable wlan capwap 1-97
1.1.66 statistics-interval 1-98
1.1.67 ten-gigabitethernet 1-99
1.1.68 tunnel encryption 1-100
1.1.69 vlan 1-102
1.1.70 wlan ap 1-103
1.1.71 wlan apdb 1-104
1.1.72 wlan apdb file 1-105
1.1.73 wlan ap-group 1-106
1.1.74 wlan ap-image-deploy 1-107
1.1.75 wlan auto-ap enable 1-108
1.1.76 wlan auto-ap persistent 1-109
1.1.77 wlan auto-persistent enable 1-110

1.1.78 wlan capwap discovery-policy unicast 1-110
1.1.79 wlan global-configuration 1-111
1.1.80 wlan image-load filepath 1-111
1.1.81 wlan re-group 1-113
1.1.82 wlan rename-ap..... 1-114
1.1.83 wlan tcp mss..... 1-114
1.1.84 wlan timezone-sync enable..... 1-115

1章 AP 管理

1.1 AP管理設定コマンド

1.1.1 ap

Syntax

ap *ap-name-list*

undo ap *ap-name-list*

デフォルト

AP 名による AP グループルールは作成されていません。

View

AP group view

定義済みユーザロール

network-admin

パラメータ

ap-name-list: スペースで区切られた最大 10 の AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別しない 1～64 文字の文字列です。

説明

ap コマンドを使用して、AP 名によるグループルールを作成します。

undo ap コマンドは、AP 名によるグループルールを削除します。

このコマンドは、指定された AP が存在するかどうかを識別しません。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP グループルールの優先順位は降順です。グループルールと一致しない AP は、デフォルトの AP グループに追加されます。

作成した AP グループルールが別の AP グループにすでに存在する場合、このコマンドはその AP グループからルールを削除します。

デフォルトの AP group view ではこのコマンドを実行できません。

例

#AP group view の下に AP 名によるグループルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap ap1 ap2 ap3

関連コマンド

- wlan ap-group

1.1.2 ap-model

Syntax

ap-model *ap-model*

undo ap-model *ap-model*

デフォルト

設定なし

View

AP group view

定義済みユーザロール

network-admin

パラメータ

ap-model: AP モデル名を指定します。

説明

ap-model コマンドは AP モデルを作成し、その view に移行します。

undo ap-model コマンドは AP モデルとその設定を削除します。

例

#AP group view で AP モデル QX-W1110 を作成し、AP group view に進みます。

<System> system-view

[System] wlan ap-group group1

[System-wlan-ap-group-group1] ap-model QX-W1110

[System-wlan-ap-group-group1-ap-model-QX-W1110]

1.1.3 bridge-aggregation

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

bridge-aggregation *interface-number*

undo bridge-aggregation *interface-number*

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、アグリゲートインタフェースは存在しません。

View

AP view

AP group AP model view

定義済みユーザロール

network-admin

パラメータ

interface-number: アグリゲートインタフェースの番号を指定します。

説明

bridge-aggregation コマンドはアグリゲートインタフェースを作成し、その view あるいは既存のアグリゲートインタフェース view に移行します。

undo bridge-aggregation コマンドはアグリゲートインタフェースを削除します。

アグリゲートインタフェースを作成したとき、システムは自動的に同一番号のアグリゲーショングループを作成します。デフォルトのアグリゲーショングループはスタティックのアグリゲーションモードです。

アグリゲートインタフェースを削除するとアグリゲートグループも削除されます。同時にアグリゲーショングループのメンバポートがアグリゲーショングループから除外されます。

リモートコンフィグレーションシンクロナイゼーションを使用すると、オンラインのすべての AP に設定が同期されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 に対してアグリゲートインタフェース 1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] bridge-aggregation 1

[AC-wlan-ap-ap1-bridge-aggregation-1]

AP グループ group1 に対してアグリゲートインタフェース 1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] bridge-aggregation 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-bridge-aggregation-1]

関連コマンド

- remote-configuration
- remote-configuration synchronize

1.1.4 data-tunnel encryption

Syntax

data-tunnel encryption { disable | enable }

undo data-tunnel encryption

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、CAPWAP データトンネル暗号化は無効です。

View

AP view

AP group view

定義済みユーザロール

network-admin

説明

CAPWAP データトンネル暗号化を有効にするには、**data-tunnel encryption enable** を使用します。

CAPWAP データトンネル暗号化を無効にするには、**data-tunnel encryption disable** を使用します。

デフォルトに戻すには、**undo data-tunnel encryption** を使用します。

この機能が有効の場合、AP は、AC から最初のキープアライブパケットを受信すると、CAPWAP 制御トンネルを介して、キーを含む暗号情報を AC と交換します。交換後、AC と AP は、CAPWAP データトンネルで送信されるデータパケットを暗号化します。キープアライブパケットは暗号化されません。

この機能により、AP は AC に再アソシエートされます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 で CAPWAP データトンネル暗号化を有効にします。

<AC> system-view

[AC] wlan ap ap1 model WA6320

[AC-wlan-ap-ap1] data-tunnel encryption enable

```
This operation will reconnect the AP. Continue? [Y/N]
```

AP group group1 で CAPWAP データトンネル暗号化を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] data-tunnel encryption enable

```
This operation will reconnect member APs that are not enabled with CAPWAP data
tunnel encryption. Continue? [Y/N]
```

関連コマンド

- tunnel encryption

1.1.5 delete file

Syntax

delete file *filename*

View

AP view

定義済みユーザロール

network-admin

パラメータ

filename: ファイル名を 1～255 文字の文字列で指定します。

説明

delete file コマンドは AP からファイルを削除します。

このコマンドは、AP がマスタ AC と CAPWAP トンネルを確立した後でのみ有効です。

例

AP ap1 から startup.cfg ファイルを削除します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] delete file startup.cfg

```
Do want to delete the flash:/startup.cfg file?[Y/N]
```

関連コマンド

- download file
- display wlan ap files

1.1.6 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

AP group view

定義済みユーザロール

network-admin

パラメータ

text: 1～64 文字で指定します。大文字、小文字を区別します。

説明

description コマンドは AP group の説明を設定します。

undo description コマンドは AP group の説明を削除します。

複数の AP グループが存在する場合は、各 AP グループの説明を設定して、AP グループを区別できます。

例

APgroup group1 の説明を設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-ap-group-group1] description L3-office

関連コマンド

- display wlan ap-group
- wlan ap-group (wlan ap-group)

1.1.7 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

AP view

定義済みユーザロール

network-admin

パラメータ

text: 1～64 文字で指定します。大文字、小文字を区別します。

説明

description コマンドは AP の説明を設定します。

undo description コマンドは AP の説明を削除します。

例

#ap 1 の説明を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-ap-ap1] description L3-office

1.1.8 display wlan ap

Syntax

display wlan ap { **all** | **name** *ap-name* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP を名前で指定します。大文字、小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

verbose: 詳細情報を表示します。

説明

display wlan ap コマンドは AP 情報を表示します。

例

#すべての AP の情報を表示します。

<AC> display wlan ap all

```
Total number of APs:1
Total number of connected APs:1
Total number of connected manual APs:1
Total number of connected auto APs:0
Total number of connected common APs:1
Total number of connected WTUs:0
Total number of inside APs:0
Maximum supported APs:2048
Remaining APs:2047
Total AP licenses:128
Local AP licenses:128
Server AP licenses:0
Remaining local AP licenses:127
Sync AP licenses:0

                          AP information

 State : I = Idle,      J  = Join,      JA = JoinAck,    IL = ImageLoad
        C = Config,    DC = DataCheck,  R  = Run   M = Master,  B = Backup

AP name                   APID  State Model         Serial ID
ap1                       1     I     QX-W1110      219801A28N819CE0002T
```

表 1-1 コマンド出力

フィールド	説明
Total number of APs	通常のAP、WT (Wireless Terminator)、WTU (Wireless Terminator Unit)を含むAPの総数
Total number of connected APs	通常のAP、WT、WTUを含む接続されたAPの総数

フィールド	説明
Total number of connected manual APs	通常のAP、WT、WTUを含む、接続された手動APの総数
Total number of connected auto APs	通常のAP、WT、WTUを含む、接続されている自動APの総数
Total number of connected common APs	接続されている通常のAPの総数
Total number of connected WTUs	接続されているWTUの総数
Maximum supported APs	Fit APおよびWTUを含むAC上のAPの最大数、WTはAP数にカウントされない
Remaining APs	残りのAP容量、つまり最大AP数から接続状態のFit APを引いた数
Total AP licenses	APライセンスの総数です。
Local AP licenses	ACローカルLicense数
Remaining local AP licenses	残りのローカルAP Licenseの数
APID	ACでAPを一意に識別するためのAPのID番号
AP name	AP名
State	APの現在の状態を以下のように表示します。 Iーアイドル Jージョイン JAージョイン確認 ILーAPがバージョンをダウンロードしています。 CーAPが初期設定をダウンロードしています。 DCーAPがデータをチェックしています。 RーAPが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。 R/Mーマスタ CAPWAPトンネルが動作しています。これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 R/Bーバックアップ CAPWAPトンネルが動作しています。これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 MーAPはマスタACに接続されています。 BーAPはバックアップACに接続されています。 R/IL:ダウンロード中のバージョンを示す
Model	APモデル情報
Serial ID	APシリアル番号。指定されていない場合はNot configuredと表示されます。

#ap 1 の詳細を表示します。

<AC> display wlan ap name ap1 verbose

```
AP name                         : ap1
AP ID                           : 1
AP group name                   : default-group
State                           : Run
Backup type                     : Master
Ready-for-Switchover            : Not ready
Online time                     : 0 days 1 hours 25 minutes 12 seconds
System uptime                   : 0 days 2 hours 22 minutes 12 seconds
Model                           : QX-6t Supported
    STBC                        : Supported
    Operational VHT-MCS Set:
        Mandatory               : Not configured
        Supported               : NSS1 0,1,2,3,4,5,6,7,8,9
                                  NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast               : Not configured
    Operational HT MCS Set:
        Mandatory               : Not configured
        Supported               : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                  10, 11, 12, 13, 14, 15
        Multicast               : Not configured
    Channel                     : 44(auto)
    Channel usage(%)            : 15
    Max power                   : -102 dBm
    Operational rate:
        Mandatory               : 6, 12, 24 Mbps
        Multicast               : Auto
        Supported               : 9, 18, 36, 48, 54 Mbps
        Disabled                : Not configured
    Distance                    : 1 km
    ANI                         : Enabled
    Fragmentation threshold     : 2346 bytes
    Beacon interval             : 100 TU
    Protection threshold        : 2346 bytes
    Long retry threshold        : 4
    Short retry threshold       : 7
    Noise Floor                 : 5 dBm
    Protection mode             : rts-cts
    MU-TxBF                     : Enabled
    SU-TxBF                     : Enabled
    Continuous mode             : N/A
    Radar-detect                : Disabled
    HT protection mode          : No protection
Radio 2:
```

```
BSSID                     : 7848-59f6-3950
State                     : Down
Radio type                : 802.11n(2.4GHz)
Antenna type              : internal
Client dot11n-only        : Disabled
Channel bandwidth         : 20/40MHz
Secondary channel offset  : SCA
Channel auto-switch       : Enabled
Short GI for 20MHz        : Supported
Short GI for 40MHz        : Supported
MIMO                      : Not Config
Green-Energy-Management   : Disabled
A-MSDU                    : Enabled
A-MPDU                    : Enabled
LDPC                      : Not Supported
STBC                      : Supported
Operational HT MCS Set:
    Mandatory             : Not configured
    Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                            10, 11, 12, 13, 14, 15, 16, 17,
                            18, 19, 20, 21, 22, 23, 24, 25,
                            26, 27, 28, 29, 30, 31
    Multicast             : Not configured
Channel                   : 5(auto)
Channel usage(%)          : 0
Max power                 : 20 dBm
Preamble type             : Short
Operational rate:
    Mandatory             : 1, 2, 5.5, 11 Mbps
    Multicast             : Auto
    Supported             : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
    Disabled              : Not configured
Distance                  : 1 km
ANI                       : Enabled
Fragmentation threshold   : 2346 bytes
Beacon interval           : 100 TU
Protection threshold      : 2346 bytes
Long retry threshold      : 4
Short retry threshold     : 7
Noise Floor               : 0 dBm
Protection mode           : rts-cts
Continuous mode           : N/A
Radar-detect              : Disabled
```

```
HT protection mode        : No protection
```

表 1-2 コマンド出力

フィールド	説明
State	APの現在の状態: ● Idle:アイドル ● Joinージョイン ● JoinAckージョイン確認 ● Imageーアップがバージョンをダウンロードしています。 ● Configーアップが初期設定をダウンロードしています。 ● Data Checkーアップがデータをチェックしています。 ● Runーアップが動作しています。これは、APとACがCAPWAPトンネルを正常に確立したことを示します。 ● R/Mーマスタ CAPWAPトンネルが動作しています。これは、APとマスタACがCAPWAPトンネルを正常に確立したことを示します。 ● R/Bーバックアップ CAPWAPトンネルが動作しています。これは、APとバックアップACがCAPWAPトンネルを正常に確立したことを示します。 ● Mーアップはマスタ ACに接続されています。 ● Bーアップはバックアップ ACに接続されています。 ● R/IL:APはオンラインであり、ACからイメージファイルをダウンロードしています。
Backup type	CAPWAPトンネルタイプ: ● Idle:トンネルが確立されていません ● Master: APとマスタAC間に確立されたCAPWAPトンネルです。 ● Backup: APとバックアップAC間に確立されたCAPWAPトンネルです。
Ready-for-Switchover	ACがAPのバックアップリンクからマスターリンクへのスイッチオーバーの準備ができているかどうか。 Ready Not ready
Region code	エリアコード
Region code lock	エリアコードロック機能: ● Enabled ● Disabled
Serial ID	APシリアル番号。シリアル番号が指定されていない場合は、Not configuredと表示されます。

フィールド	説明
MAC address	APのMACアドレス。MACアドレスが指定されていない場合は、Not configuredと表示されます。
UDP control port number	CAPWAPコントロールトンネルを確立するためにAPによって使用されるポート番号です。
UDP data port number	CAPWAPデータトンネルを確立するためにAPによって使用されるポート番号です。
H/W version	APのハードウェアバージョンです。
S/W version	APのソフトウェアバージョンです。
Boot version	APのブートバージョン
USB state	USBの状態: ● N/A ● Enabled ● Disabled
Power level	このフィールドは現在のソフトウェアバージョンではサポートされていません。 電力レベル: Low. Middle. High. 電力レベルが不明の場合、このフィールドにはN/Aが表示されます。
Power info	電源情報: ● Power adapter:ローカル電源が使用されている ● PoE (port1+port2): PoEを使用して電力を供給し、port1、port2はAPのPoE+インタフェースに電力を供給します。値は次のとおりです。 ● NA ● 802.3 af: ● 802.3 at (このフィールドのサポートは、APデバイスのモデルによって異なります。)
PoE status	PoEインタフェースの電源の状態: ● Port number:PoE ● Enabled ● Disabled (このフィールドのサポートは、AP デバイスのモデルによって異なります。)
Description	APの説明です。説明が設定されていない場合、このフィールドにはNot configuredが表示されます。

フィールド	説明
Priority	ACで設定されたAP接続の優先順位
Echo interval	APからのエコー要求の間隔
Echo count	CAPWAPトンネルキープアライブメッセージの送信回数
Keepalive interval	CAPWAPデータトンネルキープアライブメッセージの送信間隔
Discovery-response wait-time	APがDiscovery responseパケットを待機する時間
Statistics report interval	APが統計情報をエスカレーションする間隔
Fragment size (data)	CAPWAPデータパケットフラグメントの最大サイズ
Fragment size (control)	CAPWAP制御パケットの最大サイズ
MAC type	AP-AC接続のMACタイプです。 Local MAC－APはACにフレームを送信する前に802.3形式でカプセル化します。 Split MAC－APはACにフレームを送信する前に802.11形式でカプセル化します。 Local & Split MAC－APをACはフレームに送信する前に、フレームを802.3形式または802.11形式でカプセル化します。
Tunnel mode	サポートされているAPのトンネルモードです。 Local Bridging－APはローカルブリッジングをサポートし、データをACに転送しません。 802.3 Frame－APはフレームを802.3形式でカプセル化してACに送信します。 Native Frame－APはフレームを802.11形式でカプセル化してACに送信します。 Local Bridging & 802.3 Frame－APは、ローカルブリッジングモードと802.3フレームモードをサポートしています。 802.3 Frame & Native Frame－APは、802.3フレームモードとネイティブフレームモードをサポートしています。 Local Bridging & Native Frame－APはローカルブリッジモードとネイティブフレームモードをサポートしています。
CWPCAP data-tunnel status	CAPWAPデータトンネルの動作状態: ● Up ● Down

フィールド	説明
Discovery type	APの検出方法: ● Static Configuration:APは、スタティックに設定されたIPv 4またはIPv 6アドレスを使用してACを検出します。 ● DHCP:APはDHCPオプションを使用してACを検出します。 ● DNS:APはDHCP+DNSを使用してACを検出します。 ● Unknown NOTE: デュアルリンクのバックアップグループネットワークでは、バックアップACのAPはプライマリACと同じように検出されます。
Retransmission count	AC再送要求メッセージの再送回数
Retransmission interval	AC再送要求メッセージの再送間隔
Firmware upgrade	APのバージョンアップグレード: ● Enabled ● Disabled
Sent control packets	ACがRun状態の後に送信したパケットの数(Change State Event Responseメッセージを含む)
Received control packets	ACがRun状態の後に受信したパケットの数 (Change State Event Requestメッセージを含む)
Echo requests	APがRUN状態で送信したエコー要求メッセージの数
Lost echo responses	Run状態でAPが受信しなかったエコー応答メッセージの数
Average echo delay	平均エコー遅延（ミリ秒）です。

フィールド	説明
Last reboot reason	APが最後に再起動した理由: ● Power on:APデバイスの電源オフ/オン ● Hard reboot:ハード再起動 ● Watchdog reboot:ウォッチドッグによる再起動 ● Unknown reboot:原因不明の再起動 ● User soft reboot:コマンドライン、SNMP、Webなどの管理によるデバイスの再起動 ● Kernel exception soft reboot:カーネルの異常な再起動 ● Kernel deadloop soft reboot:カーネルのデッドループによる再起動 ● Auto update soft reboot:バージョンの自動アップグレードによる再起動 ● Unknown soft reboot:不明なソフトウェアによる再起動 ● Memory exhausted:メモリ不足 ● Other unknown soft reboot:その他の理由
Latest IP address	APが最後に使用したIPアドレス
Current AC IP	APオンラインの現在のACのIPアドレス
Tunnel down reason	CAPWAPトンネルがシャットダウンする原因: ● N/A:なし ● Failed to create data check timer:データタイマーの作成失敗 ● Neighbor dead timer expired:ネイバーレポートタイマーのタイムアウト ● Wait request timer expired:要求メッセージの待機タイマーのタイムアウト ● Data check timer expired:データ検出タイマーのタイムアウト ● Failed to process data channel keep-alive message:データトンネルキープアライブメッセージの処理失敗 ● Failed to process request:要求メッセージの処理失敗 ● AP was reset by admin:ユーザAPの再起動 ● AP was reset by Web :WebによるAPの再起動 ● AP was reset from OASIS:APがOASISから再起動されました。 ● WTU went offline because the WT was down:ワイヤレスターミネータがオンラインでないため、ワイヤレスターミネータユニットがオフラインになっています ● Manual AP was deleted:手動AP削除

フィールド	説明
	• Failed to come online:オンラインにできませんでした • Serial ID changed:APのSerial ID変更 • MAC address changed:APのMACアドレスの変更 • Exceeded AC max capability:AP数がACコンピテンシーセットを超えています。 • Processed join request in Run state:Run状態での処理join request • Unauthenticated AP tunnel down:認証されていないAPがオフラインになる • Failed to create AP context:APコンテキスト情報の作成に失敗しました • Received failure result code in change state event request:CAPWAP状態マシンの状態遷移中にエラー結果コードを受信しました • Failed to retransmit message:メッセージの再送信に失敗しました • Failed to download image file:APイメージのダウンロードに失敗しました • Image file downloaded successfully:APダウンロードイメージが正常にシステムを再起動しました • File operation timer expired:ファイル操作タイマーのタイムアウト • Failed to add tunnel:トンネルの追加に失敗しました • Received WTP tunnel down event from AP:ACがAPのトンネルダウンイベントを受信した場合 • Backup AC closed the backup tunnel:バックアップACはバックアップトンネルを閉じます。 • Master and backup tunnel switchover:プライマリトンネルスイッチオーバー • Failed to inherit configuration:構成の継承に失敗しました • AP authentication failed:AP認証に失敗しました • Backup AP upgrade failed:バックアップトンネルAPのアップグレードに失敗しました • Board is inactive:ボードの非アクティブ状態 • WT went offline:ワイヤレスターミネータがダウンしました • Lack of AP license:AP数なしLicense • WAP went offline because the SPM was down:SPMダウンリンクによるWAPダウンリンク

フィールド	説明
	• SPM was down:SPMオフライン • Encryption status mismatch :暗号化の実行状態と構成状態が矛盾しています • Associated local AC went down:Local ACオフラインが原因でAPがオフラインになる • AP was reset due to inconsistent local and reported radio statistics :Radioデータ統計エスカレーションデータの不一致 • AP was reset due to inconsistent AP state on APMGR and lib:APMGRとlib側APの状態の不一致 • AP was reset due to inconsistent BSS state on AC and AP:ACとAPのBSS状態の不一致 • APs failed to request a license:バックアップトンネルAPのアップグレード時にLicenseが失敗する • WT status is incorrect in master and backup switchover in dual link backup:バックアップトンネルワイヤレスターミネータの状態アップグレード時に依存するワイヤレスターミネータの状態がプライマリトンネルではありません • Master and backup switchover is not allowed if AP software upgrade is enabled and APs were logged off:APアップグレードスイッチがオンのときにリンクスイッチが許可されず、APが強制的にオフラインになる • WTU creation timer timed out after a master and backup switchover in dual link backup: ワイヤレス ターミネーターバックアップがマスターにアップグレードされた後、作成遅延チェックのワイヤレス ターミネーター アップグレード タイマーがタイムアウトします。
Connection count	APとACの接続数がゼロになるのは、次の場合のみです。 • ACの再起動 • APシリアル番号の変更 reset wlan apコマンドを使用しても、AP接続がゼロにならないことに注意してください。
Backup IPv4	バックアップACのIPv 4アドレス。指定しない場合は、Not configuredと表示されます。
Backup IPv6	バックアップACのIPv 6アドレス。指定しない場合は、Not configuredと表示されます。
Ctrl-tunnel encryption	• Enabled • Disabled

フィールド	説明
Ctrl-tunnel encryption state	• Encrypted:暗号化 • Not encrypted:暗号化されていません
Data-tunnel encryption	• Enabled • Disabled
Data-tunnel encryption state	• Encrypted • Not encrypted
LED mode	LED点灯モードです。 quietーすべてのLEDがオフです。 awakeーすべてのLEDを1分毎に点灯します。 always-onーすべてのLEDは常にオンです。 normalー本モードでのLED点灯の仕方は、APモデルによって変わります。
Remote configuration	• Enabled • Disabled
Radio	無線周波数
BSSID	RadioのMACアドレス。N/Aは、APがACとCAPWAPトンネルを確立していないことを示します。
State	Radioステータス: • Up • Down
Radio type	ワイヤレスモードです。 2.4 GHz 802.11b 802.11g 802.11n(2.4GHz) 5 GHz 802.11a 802.11n(5GHz) 802.11ac 80.211ax
Antenna type	アンテナタイプ
Client dot11ax-only	Enableー802.11a/b/g/n/axクライアントを無線と関連付けることができます。 Disableー802.11axクライアントだけを無線に関連付けることができます。
Client dot11ac-only	Enableー802.11a/b/g/n/acクライアントを無線と関連付けることができます。 Disableー802.11acクライアントだけを無線に関連付けることができます。

フィールド	説明
Client dot11n-only	Enable－802.11a/b/g/n/ac/axクライアントを無線と関連付けることができます。 Disable－802.11nまたは802.11ac/axクライアントだけを無線に関連付けることができます。
Channel bandwidth	チャネル帯域幅: ● 20 MHz ● 20/40 MHz ● 20/40/80 MHz ● 20/40/80/160 MHz ● 20/40/80/160/(80+80) MHz
Operatingbandwidth	無線動作帯域幅
Channel auto-switch	20/40M帯域幅自動切り替えがオンになっている場合にのみ表示される現在の帯域幅の値は、Beaconフレームの帯域幅と同じです。
Secondary channel offset	802.11nおよび802.11ac/ax無線モードのセカンダリチャネル情報です。 SCA(Second Channel Above)－APは40 MHz帯域幅モードで動作し、セカンダリチャネルはプライマリチャネルよりも上にあります。 SCB(Second Channel Below)－APは40 MHz帯域幅モードで動作し、セカンダリチャネルはプライマリチャネルよりも下にあります。 SCN－APは40 MHz帯域幅モードでは動作しません。 このフィールドは、無線が使用している帯域幅が20/40/80 MHzの場合にのみ使用できます。
Secondary channel center frequency	802.11 ac無線周波数モードで、無線周波数の動作帯域幅が160/(80+80) MHzの場合、補助チャネルは80 M帯域幅の中心周波数情報に位置する。 (このフィールドは、160/(80+80) MHzの帯域幅でのみサポートされます。)
Short GI for 20MHz	無線周波数帯域幅が20 MHzの場合、Short GIのサポートは次のとおりです。 Not supported Supported
Short GI for 40MHz	無線周波数帯域幅が40 MHzの場合、Short GIのサポートは次のとおりです。 ● Not supported ● Supported

フィールド	説明
Short GI for 80MHz	無線周波数帯域幅が80 MHzの場合、Short GIのサポートは次のとおりです。 ● Not supported ● Supported
Short GI for 160MHz	無線周波数帯域幅が160 MHzの場合、Short GIのサポートは次のとおりです。 ● Not supported ● Supported
mimo	mimo機能: ● 1 x 1:無線周波数は1つのストリームトランシーバーモードで動作 ● 2 x 2:無線周波数は2つのストリームトランシーバーモードで動作 ● 3 x 3: 無線周波数は3つのストリームトランシーバーモードで動作 ● 4 x 4:無線周波数は4つのストリームトランシーバーモードで動作 ● 5 x 5: 無線周波数は5つのストリームトランシーバーモードで動作 ● 6 x 6: 無線周波数は6つのストリームトランシーバーモードで動作 ● 7 x 7:7つのストリームモードで動作する無線周波数 ● 8 x 8無線周波数は:8つのストリームトランシーバーモードで動作 ● Not configured:デフォルト設定を使用 ● (PowerLow):上記の9つのモードの後にこの表示がある場合、APの電力レベルが低いことを示します。無線周波数は1つのストリームトランシーバーモードでのみ動作できます。
Green-Energy-Management	Disabled ● Enabled
A-MSDU	● Disabled ● Enabled
A-MPDU	● Disabled ● Enabled
LDPC	● Supported:無線周波数はLDPC機能をサポート ● Not Supported:無線周波数はLDPC機能をサポートしていません

フィールド	説明
STBC	● Supported ● Not Supported
Operational HE-MCS Set	Supported－サポートMCSセット Mandatory－必須MCSセット Multicast－マルチキャストMCSセット
Operational VHT MCS Set	Supported－サポートVHT MCSセット Mandatory－必須VHT MCSセット Multicast－マルチキャストVHT MCSセット
Operational HT MCS Set	Supported－サポートHE MCSセット Mandatory－必須HE MCSセット Multicast－マルチキャストHE MCSセット
Channel	現在のチャネルがAPによって自動的に選択された最適なチャネルである場合、このフィールドには Number<auto>が表示されます。 現在のチャネルが手動で設定されている場合、このフィールドにはNumberが表示されます。 現在のチャネルがレーダー信号を避けるためにAPによって自動的に選択されたチャネルである場合、このフィールドにはNumber<avoid radar>と表示されます。
Channel usage (%)	チャネル使用率
Max power	無線の最大送信電力です。
Preamble type	プリアンブルの種類: ● Long ● Short
Operational rate	Mandatory Supported Multicast Disable Not configured
Distance	無線信号が到達できる最大距離です。
ANI	ANI機能の状態: ● Enabled ● Disable
Fragmentation threshold	フレームのフラグメンテーションしきい値
Beacon interval	Beaconフレームを送信する間隔
Protection threshold	保護メカニズムを起動するために必要なフレーム長のしきい値です。
Long retry threshold	長さがRTSしきい値を超えたフレームの最大再送試行回数です。

フィールド	説明
Short retry threshold	長さがRTSしきい値を超えないフレームの最大再送試行回数です。
Frame aging time in cache	フレームがキャッシュに保存される最大時間
Noise Floor	ノイズベース
Smart antenna	スマートアンテナ機能: ● Enabled ● Disabled (このフィールドのサポートは、APデバイスのモデルによって異なります。)
Smart antenna policy	スマートアンテナポリシー: ● Auto ● High availability ● High throughput (このフィールドのサポートは、APデバイスのモデルによって異なります。)
Protection mode	競合回避モード: ● cts-to-self ● rts-cts
MU-TxBF	MUTxBF機能: ● Enabled ● Disabled (このフィールドのサポートは、AP デバイスのモデルによって異なります。)
SU-TxBF	SUTxBF機能: ● Enabled ● Disabled (このフィールドのサポートは、AP デバイスのモデルによって異なります。)
Continuous mode	通常モードで使用されるレート、MCSインデックス値、NSSインデックス値、およびVHT-MCSインデックス値。N/Aは通常モードが構成されていないことを示します。
OFDMA random access RUs	HEランダムアドレスのサポート ● Supported ● Not Supported

フィールド	説明
DL-OFDMA	ダウンリンクOFDMA機能: ● Enabled ● Disabled (このフィールドのサポートは、APデバイスのモデルによって異なります。)
UL-OFDMA	アップリンクOFDMA機能: ● Enabled ● Disabled (このフィールドのサポートは、AP デバイスのモデルによって異なります。)
UL-MU-MIMO	アップリンクMU-MIMO機能: ● Enabled ● Disabled (このフィールドのサポートは、APデバイスのモデルによって異なります。)
BSS-COLOR	BSS-COLOR機能: Enabled Disabled (このフィールドのサポートは、AP デバイスのモデルによって異なります。)
TWT negotiation	TWTネゴシエーション機能の状態: Enabled Disabled (このフィールドのサポートは、APデバイスのモデルによって異なります。)
Radar-detect	レーダー検出機能: Enabled Disabled

フィールド	説明
HT protection mode	802.11n保護モード: No protection APに関連付けられたクライアントと近接の無線装置は802.11nモードで動作しています。APに関連付けられたクライアントは40MHz帯で動作しています。 APに関連付けられたクライアントは802.11nモードで動作しています。APに関連付けられたクライアントは40MHz帯で動作しています。 Non-member protection すべてのAPに関連付けられたクライアントは802.11nモードで動作しています。近接の無線装置は非802.11nモードで動作しています。 20 MHz protection APの無線は40MHz帯を使用します。APに関連付けられたクライアントと近接の無線装置は802.11nモードで動作しています。20MHzの帯域幅を持つ最低 1 つのクライアントがAPの無線と関連付けられています。 Non-HT mixed 上記のいずれのモードにもあてはまらないときに使用するモードです。

1.1.9 display wlan ap address

Syntax

display wlan ap { **all** | **name** *ap-name* } **address**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP を名前で指定します。大文字、小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

説明

display wlan ap address コマンドは AP アドレス情報を表示します。

例

すべての AP のアドレス情報を表示します。

<AC> display wlan ap all address

```
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of inside APs: 0

AP name                      IP address                MAC address
ap1                          1.1.1.5                   000b-6b8f-fc6a
```

表 1-3 コマンド出力

フィールド	説明
Total number of APs	通常のAP、WT (Wireless Terminator、ワイヤレスターミネータ)、WTU (Wireless Terminator Unit、ワイヤレス終端ユニット)を含むAPの数
Total number of connected APs	通常のAP、WT、WTUを含む接続されたAPの総数
Total number of connected manual APs	通常のAP、WT、WTUを含む、接続された手動APの総数
Total number of connected auto APs	通常のAP、WT、WTUを含む、接続されている自動APの総数
AP name	AP名
IP address	APのIPアドレス。APがオンラインになっていない場合、このフィールドにはN/Aと表示されます。
MAC address	APのMACアドレス。APがオンラインになっていない場合、このフィールドにはN/Aと表示されます。

1.1.10 display wlan ap all feature capwap

Syntax

display wlan ap all feature capwap

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap all feature capwap コマンドは、CAPWAP トンネルの設定状態を表示します。

例

#CAPWAP トンネルの設定状態を表示します。

<AC> display wlan ap all feature capwap

```
AP name                Upgrade   Encryption  Control-address   Switch-back
ap1                    Disabled Both       Enabled          Disabled
```

表 1-4 コマンド出力

フィールド	説明
Upgrade	APソフトウェアアップグレード • Enabled • Disabled
Encryption	CAPWAPトンネルの暗号化です。 • Control—制御トンネルの暗号化が有効です。 • Data—データトンネルの暗号化が有効です。 • Both—制御、データの両方のトンネルの暗号化が有効です。 • Disabled—制御、データの両方のトンネルの暗号化が無効です。
Control Address	(未サポート) AC再検出: • Enabled • Disabled
Switch back	(未サポート) AC階層のCAPWAPトンネルスイッチバック機能: • Horizontal • Vertical • Disabled • Both

1.1.11 display wlan ap connection-record

Syntax

display wlan ap { **all** | **name** *ap-name* } **connection-record**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての AP の接続レコードを表示します。

name *ap-name*:指定した AP の接続レコードを表示します。*ap-name* は AP 名を表します。1~64 文字の文字列で、英数字、アンダースコア、「.」 、[」 、「]、「/」 、「-」を使用でき、大文字と小文字が区別されます。

説明

display wlan ap connection-record コマンドを使用して、AC 上の AP 接続レコードを表示します。

例

#AC 上のすべての AP の接続レコードを表示します。

<AC> display wlan ap all connection-record

```
AP name                    IP address     State    Time
ap2                        192.168.100.27 Run      01-06 09:06:40
```

表 1-5 コマンド出力

フィールド	説明
State	APの状態: ● Discovery:AP検出ACフェーズ ● Join:CAPWAPトンネル確立状態 ● Offline:オフラインステータス ● Run:CAPWAPトンネルが実行状態
Time	最後にCAPWAPトンネルを確立した時刻

1.1.12 display wlan ap diagnostic-information

Syntax

display wlan ap name *ap-name* **diagnostic-information**

View

すべての view

定義済みユーザロール

network-admin

パラメータ

name *ap-name*：AP の名前を指定します。*ap-name* は AP 名を示します。これは 1 ～ 64 文字の文字列であり、文字、数字、アンダースコア、「.」、「[」、「」」を含めることができます。]"、"/"、"-" は大文字と小文字が区別されます

説明

AP 診断情報を AC に保存するには、**display wlan ap diagnostic-information** を使用します。

このコマンドを使用すると、AP が AC に診断情報を報告できます。AP にログインしなくても、AC のストレージメディアから診断情報ファイルを表示または削除できます。

このコマンドを実行すると、AP は診断情報ファイルを生成し、AC のストレージメディアの/apdiag/apdiag_ap1.tar.gz ディレクトリに送信してから、ローカル診断情報ファイルを削除します。

報告する診断情報タイプを設定するには、**display diagnostic-information** コマンドを使用します。この機能は、オンライン AP でのみ有効です。

例

ap1 の AP 診断情報を AC に保存します。

<AC> display wlan ap name ap1 diagnostic-information

```
Diagnostic information is being output to flash:/apdiag/apdiag_ap1.tar.gz.
Saved successfully.
```

1.1.13 display wlan ap files

Syntax

display wlan ap name *ap-name* **files**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *ap-name* : AP の名前を指定します。*ap-name* は AP 名を示します。これは 1 ～ 64 文字の文字列であり、文字、数字、アンダースコア、「.」、「[」、「」」を含めることができます。]"、"/"、"-" は大文字と小文字が区別されます

説明

display wlan ap files コマンドは、AP 上のファイルとフォルダの情報を表示します。

例

#ap 1 のファイルおよびフォルダ情報を表示します。

<AC> display wlan ap name ap1 files

```
Directory of flash:
   0   13638656  wa4300-system.bin
   1   2573312   wa4300-boot.bin
131072 KB total (114208 KB free)
```

表 1-6 コマンド出力

フィールド	説明
Directory of	現在表示されているAPディレクトリ
013638656xx.xx	APフォルダの情報: • 0は番号で、システムによって自動的に割り当てられます。 • 13638656はファイルサイズで、単位はBです。「-」と表示されている場合は、フォルダであることを示します。 • xx.xxは名前です。

関連コマンド

- download file
- delete file

1.1.14 display wlan ap online-time

Syntax

display wlan ap { **all** | **name** *ap-name* } **online-time**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP を名前で指定します。大文字、小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

説明

display wlan ap online-time コマンドは AP のオンライン期間を表示します

例

すべての AP のオンライン期間を表示します。

<AC> display wlan ap all online-time

```
AP name          IP address            Time
ap1              1.1.1.2               0 days 0 hours 2 minutes 6 seconds
ap2              1.1.1.1               0 days 0 hours 5 minutes 6 seconds
ap3              1.1.1.6               0 days 0 hours 2 minutes 1 seconds
```

表 1-7 コマンド出力

フィールド	説明
AP name	AP名
IP address	APのIPアドレス
Time	APがオンラインになってからのAPのリアルタイムアソシエーション期間です。

1.1.15 display wlan ap reboot-log

Syntax

display wlan ap name *ap-name* **reboot-log**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *ap-name*: AP を名前で指定します。大文字、小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

説明

display wlan ap reboot-log コマンドは AP の再起動のログを表示します。

AP でシステムクラッシュが発生した場合、このコマンドを使用してクラッシュに関する詳細情報を表示できます。

このコマンドを使用するには、指定した AP が Run 状態であることを確認してください。

例

#ap 1 の再起動ログ情報を表示します。

<AC> display wlan ap name ap1 reboot-log

```
Debugging information is not available on the AC.
Downloading debugging data from AP. Continue? [Y/N]:y
Downloading debugging data. Please wait...
Please enter the same command again to view the log messages.
```

<AC> display wlan ap name ap1 reboot-log

```
---------------------- Reboot record 1 ----------------------
Recorded at          : 2018-07-20  03:29:43.324529
Occurred at          : 2018-07-20  03:29:43.324529
Reason              : 0x8
Thread              : devd (TID: 50)
Context             : thread context
Cpu                : 0
Kernel module info    : module name (system) module address (0xd145a000)
                      module name (addon) module address (0xd00d5000)
Last 5 thread switches : WDRVFwdKthread (3:29:43.323999)-->
                       swapper (3:29:43.324011)-->
                       WDRVFwdKthread (3:29:43.324467)-->
                       swapper (3:29:43.324478)-->
                       devd (3:29:43.324502)-->
```

…

関連コマンド

- **reset wlan ap reboot-log**

1.1.16 display wlan ap region-code

Syntax

display wlan ap { all | name ap-name } region-code

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP を名前で指定します。大文字、小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

verbose: 詳細情報を表示します。

説明

all: 全ての AP を指定します。

name *ap-name* : ＡＰ 名 を指定します。 AP 名は、文字、数字、アンダースコア（ （_）、ドット（ （.）、左括弧 （[）、右括弧 （]）、スラッシュ （/）、ハイフン （-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

例

すべての AP の地域コード情報を表示します。

<AC> display wlan ap all region-code

Region Code

AP name	Region Code
ap1	JP JAPAN
ap2	JP JAPAN
ap3	JP JAPAN

表 1-8 コマンド出力

フィールド	説明
Region Code	地域コード

1.1.17 display wlan ap running-configuration

Syntax

display wlan ap { **all** | **name** *ap-name* } **running-configuration** [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

name *ap-name*: AP を名前で指定します。大文字、小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

verbose: 詳細情報を表示します。

説明

display wlan ap running-configuration コマンドは指定した AP またはすべての AP のランニングコンフィグレーションを表示します。

例

#すべての AP の詳細なランニングコンフィグレーションを表示します。

<AC> display wlan ap all running-configuration verbose

```
(i) -- Inherited from AP group
(g) -- Inherited from AP global-configuration
(wt)-- Inherited from WT


#
wlan ap ap1 model QX-W1110 id 5
  ap group name 1
  serial-id 219801A28N819CE00021
  region code 156
```

```
  echo interval 10 (i)
  retransmission count 3 (i)
  retransmission interval 5 (i)
  statistics interval 50 (i)
  fragment-size data 1500 (i)
  fragment-size control 1450 (i)
  tunnel-preempt disable (g)
  firmware-upgrade disable (g)
  priority 4 (i)
……


  radio 1
    radio type 802.11ac (i)
    radio disable (i)
    channel auto<64> (i)
    channel unlock (i)
    fragment-threshold 2346 (i)
    max-power 20 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
……


radio 2
    radio type 802.11n(2.4GHz) (i)
    radio disable (i)
    channel auto<11> (i)
    channel unlock (i)
    fragment-threshold 2346 (i)
    max-power 20 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
……


#
wlan ap ap2 model QX-W1110 id 6
  ap group name 2
  serial-id 219801A28N819CE0002T
  region code 156
  echo interval 10 (i)
```

```
  retransmission count 3 (i)
  retransmission interval 5 (i)
  statistics interval 50 (i)
  fragment-size data 1500 (i)
  fragment-size control 1450 (i)
  tunnel-preempt disable (g)
  firmware-upgrade disable (g)
  priority 4 (i)
……

  radio 1
    radio type 802.11ac (i)
    radio disable (i)
    channel auto<60> (i)
    channel unlock (i)
    fragment-threshold 2346 (i)
    max-power 20 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
……

  radio 2
    radio type 802.11n(2.4GHz) (i)
    radio disable (i)
    channel auto<13> (i)
    channel unlock (i)
    fragment-threshold 2346 (i)
    max-power 20 (i)
    power unlock (i)
    distance 1 kilometer (i)
    ANI Enabled (i)
……
```

1.1.18 display wlan ap statistics association-failure-record

Syntax

display wlan ap statistics association-failure-record

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap statistics association-failure-record コマンドは AP の関連付けに失敗した記録を表示します。

例

AP の関連付けに失敗した記録を表示します。

<AC> display wlan ap statistics association-failure-record

```
MAC address    AP ID Last failed at   Reason
9a48-45ed-0300 12312 07-07/15:56:25   AP authentication failed
```

表 1-9 コマンド出力

フィールド	説明
MAC address	APのMACアドレス
AP ID	ACでAPを一意に識別するためのAPのID
Last failed at	APがACと関連付けられた最後の時間です。フォーマットはdate/hh:mm:ssです。

フィールド	説明
Reason	関連づけに失敗した理由です。 メモリ不足。 APが存在しません。 APのライセンス不足。 MACアドレスが使用されています。 APLBの追加に失敗しました。 APが別のACを選択しました。 ACでAPの最大数に到達しました。 Run状態の加入要求を受信しました。 APLBチェックに失敗しました。 HA smoothのAPアクセスに拒否されました。 AP認証に失敗しました。 Auto APの作成に失敗しました。 手動APオンラインinfoチェックに失敗しました。 インデックスの追加に失敗しました。 APとACのバージョンがあっていません。 要求待ちタイマが終了しました。 失敗リザルトコードを受信しました。 トンネルの追加に失敗しました。 APの設定が見つかりません。 AP IDが一致していません。 APの基本ランニングデータの追加に失敗しました。 一貫性のないAP ID。 クエリメッセージの送信に失敗しました。 イメージファイルを開くタイマの有効期限が切れました。

1.1.19 display wlan ap statistics cloud-cluster switch-over-state

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでサポートしています。

Syntax

display wlan ap statistics cloud-cluster switch-over-state [**history**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

history：マスタ､スタンバイの切り替わりに関連したフラグビットのログを表示します。

説明

display wlan ap statistics cloud-cluster switch-over-state コマンドはクラウドクラスタのマスタ、スタンバイが切り替わる際のフラグビットの状態を表示します。このコマンドの表示によりマスタ、スタンバイの現在の論理プロセスを判断できます。

このコマンドを使用して、クラウドクラスタフラグビットのステータス、設定時間、および反転時間を表示し、マスタ、スタンバイ切り替わりの現在のロジックプロセスを確認します。

例

クラウドクラスタでのマスタ、スタンバイ切り替えプロセス中のフラグビットのステータスを表示します。

<AC> display wlan ap statistics cloud-cluster switch-over-state

```
Switch-over flag    Current value  Last change at
AgentRespEnable     FALSE          03-21/07:57:38
UpgradingFlag       FALSE          03-21/07:57:36
DenyApOnline        FALSE          03-21/07:57:38
CurrentMasterLIP    8              03-21/07:57:37
```

表 1-10 コマンド出力

フィールド	説明
Switch-over flag	マスタ、スタンバイ切り替えフラグビット。使用可能なフラグビットは次のとおりです。 AgentRespEnable－エージェント応答フラグ。メインボードが取り外された場合のコールドスタンバイ中、またはボードが取り外された場合のホットスタンバイ中にアクティブ化されます。この間、APの切断を防ぐためにCAPWAPトンネル応答エージェントがアクティブ化されます。コマンド展開を遮断するために使用できます。このフラグは、マスタ、スタンバイ切り替わり中またはボードが取り外された場合に有効に設定され、マスタ、スタンバイ切り替わりの完了後に無効に設定されます。 UpgradingFlag－アップグレードフラグ。マスタ、スタンバイ切り替わり中にアクティブ化されます。このフラグは、スタンバイデバイスの初期化が開始されると有効に設定され、マスタ、スタンバイ切り替わりの完了後に無効に設定されます。 DenyApOnline－アソシエーション拒否フラグ。マスタ、スタンバイ切り替わりプロセス中にAPアソシエーションを代行受信するために使用されます。このフラグは、スタンバイ装置の初期化が開始されると有効に設定され、マスタ、スタンバイ切り替わりの完了後に無効に設定されます。 CurrentMasterLIP－現在のマスタ装置のボード番号。
Current value	フラグによって表される機能のステータスを示すフラグの現在の値。AgentRespEnable、UpgradingFlag、およびDenyApOnlineの値はTRUEまたはFALSEです。TRUEはEnabledを表し、FALSEはDisabledを表します。CurrentMasterLIPの場合、このフィールドには現在のマスタ装置のボード番号が表示されます。
Last change at	フラグビット値が最後に変更された時刻。

クラウドクラスタでのマスタ、スタンバイ切り替えプロセス中のフラグビットのログを表示します。

<AC> display wlan ap statistics cloud-cluster switch-over-state history

```
Switch-over flag     : AgentRespEnable
```

```
Current value       : FALSE
History:
10-10/15:51:27 : FALSE
10-10/15:50:12 : TRUE
-------------------------------------------------
Switch-over flag    : UpgradingFlag
Current value       : FALSE
History:
10-10/15:53:11 : FALSE
10-10/15:52:22 : TRUE
-------------------------------------------------
Switch-over flag    : DenyApOnline
Current value       : TRUE
History:
10-10/15:56:21 : TRUE
10-10/15:55:33 : FALSE
-------------------------------------------------
Switch-over flag    : CurrentMasterLIP
Current value       : 8
History:
     03-21/07:57:36 : 8
```

表 1-11 コマンド出力

フィールド	説明
Switch-over flag	マスタ、スタンバイ切り替えフラグビット。使用可能なフラグビットは次のとおりです。 AgentRespEnable－エージェント応答フラグ。メインボードが取り外された場合のコールドスタンバイ中、またはボードが取り外された場合のホットスタンバイ中にアクティブ化されます。この間、APの切断を防ぐためにCAPWAPトンネル応答エージェントがアクティブ化されます。コマンド展開を遮断するために使用できます。このフラグは、マスタ、スタンバイ切り替わり中またはボードが取り外された場合に有効に設定され、マスタ、スタンバイ切り替わりの完了後に無効に設定されます。 UpgradingFlag－アップグレードフラグ。マスタ、スタンバイ切り替わり中にアクティブ化されます。このフラグは、スタンバイデバイスの初期化が開始されると有効に設定され、マスタ、スタンバイ切り替わりの完了後に無効に設定されます。 DenyApOnline－アソシエーション拒否フラグ。マスタ、スタンバイ切り替わりプロセス中にAPアソシエーションを代行受信するために使用されます。このフラグは、スタンバイ装置の初期化が開始されると有効に設定され、マスタ、スタンバイ切り替わりの完了後に無効に設定されます。 CurrentMasterLIP－現在のマスタ装置のボード番号。
Current value	フラグによって表される機能のステータスを示すフラグの現在の値。AgentRespEnable、UpgradingFlag、およびDenyApOnlineの値はTRUEまたはFALSEです。TRUEはEnabledを表し、FALSEはDisabledを表します。CurrentMasterLIPの場合、このフィールドには現在のマスタ装置のボード番号が表示されます。
History	フラグビットのログ。

1.1.20 display wlan ap statistics image-download

Syntax

display wlan ap statistics image-download [failed | in-progress | succeeded]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

failed: イメージのダウンロードに失敗した AP を表示します。

in-progress: イメージをダウンロード中の AP を表示します。

succeeded: イメージのダウンロードが成功した AP を表示します。

説明

display wlan ap statistics image-download コマンドは AP イメージのダウンロード情報を表示します。パラメータを指定しない場合、AP イメージのダウンロードに関する簡易情報を表示します。

例

AP イメージのダウンロードに関する簡易情報を表示します。

<AC> display wlan ap statistics image-download

```
Completed                                  : 50%
Time consumed                               : xxd hh:mm:ss
Max. concurrent image downloads of online APs : 192
AP count:
 Total to download : 300
 Succeeded : 152
 In-progress : 140
 Failed : 8
```

表 1-12 コマンド出力

フィールド	説明
Completed	イメージのダウンロードが完了したAPの割合です。
Time consumed	イメージのダウンロードにかかった時間です。
Total to download	ソフトウェアを更新する必要があるAPの合計数です。
Succeeded	イメージのダウンロードに成功したAPの数です。
In-progress	イメージをダウンロード中のAPの数です。
Failed	イメージのダウンロードに失敗したAPの数。

AP イメージをダウンロード中の AP を表示します。

<AC> display wlan ap statistics image-download in-progress

```
AP name                    Time consumed
ap6                            xxd 00:45:11
ap7                            N/A
ap8                            xxd 00:14:05
ap9                            xxd 01:16:09
....
------More----
```

表 1-13 コマンド出力

フィールド	説明
Time consumed	イメージのダウンロードにかかった時間です。 イメージをダウンロードしていない場合、このフィールドにはN/Aと表示されます。

AP イメージのダウンロードが失敗した AP を表示します。

<AC> display wlan ap statistics image-download failed

```
AP name                  Failure reason
ap1                     Tunnel down
ap2                     AP memory not enough
ap3                     Image file does not exist
ap5                     Others(0x40010001)
....
------More----
```

表 1-14 コマンド出力

フィールド	説明

Failure reason	失敗理由
	• Tunnel down.
	• AP memory not enough.
	• Image file does not exist.
	• Retransmission failed.
	• Time out.
	• Others—エラーコードは括弧で囲まれています。エラーコードのオプションは次のとおりです。
	  • 0x40010001—APイメージのダウンロードに失敗しました。
	  • 0x622c0085—接続が終了しました。

AP イメージのダウンロードが成功した AP を表示します。

<AC> display wlan ap statistics image-download succeeded

```
AP name                  Version
ap1                      R5220
ap2                      R5220
ap3                      R5220
ap5                      R5220
....
------More----
```

1.1.21 display wlan ap statistics online-record

Syntax

display wlan ap statistics online-record [**datetime** *date time* [**count** *count*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

datetime date time:オンライン AP 数量レコードを表示する開始時刻を指定します。date 引数は、YYYY/MM/DD 形式で日付を表します。YYYY の値の範囲は 2000 から 2035 です。MM の値の範囲は 1 から 12 です。DD の値の範囲は月によって異なります。time 引数は、時刻を hh:mm 形式で表します。hh の値の範囲は 0 から 23 です。mm の値の範囲は 0 から 59 です。このオプションを指定しない場合、過去 7 日間のオンライン AP 数量に関するすべての統計情報が時間の降順で表示されます。

count *count*:表示するオンライン AP 数量レコードの数を 1 から 256 の範囲で指定します。このオプションを指定しない場合、10 のオンライン AP 数量レコードが表示されます。

説明

display wlan ap statistics online-record コマンドはオンライン AP 数の記録を表示します。

オンライン AP 数の記録は 1 分間隔で 1 つずつ表示されます。コマンドは過去 7 日間で生成された記録を表示します。*time* パラメータを指定した場合、指定した時間から生成された記録を表示します。

例

2017/10/11 10:25 後に生成されたオンライン AP 数の記録を 11 表示します。

<AC> display wlan ap statistics online-record time 2017/10/11 10:16:11 count 11

```
Time                 Manual APs      Auto APs       Total       Total delta
2017-10-11 10:16:00        20             10            30          -2
2017-10-11 10:17:00        22             10            32          +6
2017-10-11 10:18:00        16             10            26          0
2017-10-11 10:19:00        16             10            26          0
2017-10-11 10:20:00        16             10            26          0
2017-10-11 10:21:00        16             10            26          0
2017-10-11 10:22:00        16             10            26          0
2017-10-11 10:23:00        16             10            26          0
2017-10-11 10:24:00        16             10            26          0
2017-10-11 10:25:00        16             10            26          0
2017-10-11 10:26:00        16             10            26          0
```

表 1-15 コマンド出力

フィールド	説明
Time	時間
Manual APs	手動APオンライン数
Auto APs	自動アクセスポイントのオンライン数
Total	オンラインAPの総数
Total delta	直前の1分間と比較したAPオンライン数の変化

1.1.22 display wlan ap-group

Syntax

display wlan ap-group [**brief** | **name** *group-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

brief: すべての AP group に関する簡易情報を表示します。

name *group-name*: 指定した AP group に関する詳細情報を表示します。group-name 引数は、1～31 文字の大文字小文字を区別しない AP group の名前を表します。

説明

display wlan ap-group コマンドはすべての AP group または指定した AP group に関する情報を表示します。

パラメータを指定しない場合、このコマンドはすべての AP group に関する詳細情報を表示します。

例

すべての AP group に関する詳細情報を表示します。

[AC] display wlan ap-group

```
Total number of AP groups: 2
AP group name      : default-group
Description        : Not configured
AP model           : Not configured
APs                : Not configured
AP group name      : group1
Description        : abcd
AP model           : QX-W1110
AP grouping rules:
  AP name          : ap1, ap2
  Serial ID        : 219801A28N819CE0002T
  MAC address      : 0AFB-423B-893C
  IPv4 address     : Not configured
  IPv6 address     : Not configured
APs                : ap1 (AP name)
```

AP group group1 に関する詳細情報を表示します。

<AC> display wlan ap-group group1

```
AP group name      : group1
Description        : Not configured
AP model           : QX-W1110
AP grouping rules:
  AP name          : ap1, ap2
  Serial ID        : 219801A28N819CE0002T
  MAC address      : 0AFB-423B-893C
  IPv4 address     : Not configured
  IPv6 address     : Not configured
APs                : ap1 (AP name)
```

すべての AP group に関する簡易情報を表示します。

<AC> display wlan ap-group brief

```
Total number of AP groups: 4
AP group name               Group ID  Member APs   Online APs
default-group               1         1            0
group1                      2         2006         1986
group2                      3         10           10
group3                      4         4            4
```

表 1-16 コマンド出力

フィールド	説明する
Total number of AP groups	APグループの合計数
AP group name	APグループ名
Description	APグループの説明
AP model	APモデル名
AP grouping rules	APグループルール
AP name	AP名前のグループ化規則
Serial ID	APシリアル番号のグループ化ルール
MAC address	AP MACアドレスグルーピング規則
IPv4 address	IPv 4セグメントイングループルール
IPv6 address	(未サポート) IPv 6セグメントイングループ規則
AP	APグループ内のAP
Group ID	ACでAPグループを一意に識別するためのAPグループのID番号
Member APs	このAPグループに参加するAPの数
Online APs	このAPグループ内のオンラインAPの数

関連コマンド

- wlan ap-group

1.1.23 display wlan ap-model

Syntax

display wlan ap-model { **all** | **name** *model-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP モデルを指定します。

name *model-name*: AP モデルの名前を指定します。

説明

display wlan ap-model コマンドは AP モデル情報を表示します。

例

#AP モデル QX-W1110 の情報を表示します。

<AC> display wlan ap-model name QX-W1110

```
AP model       : QX-W1110
Alias          : QX-W1110
Vendor name    : NEC
Vendor ID      : 25506
License weight  : 100
License type    : 1
Radio count    : 2
 Radio 1:
  Mode         : 802.11a, 802.11an, 802.11ac
  Default mode  : 802.11ac
  BSS count     : 16
 Radio 2:
  Mode         : 802.11b, 802.11g, 802.11gn
  Default mode  : 802.11gn
  BSS count     : 16
Version Support List :
 Hardware Version Ver.A:
  Software Version        : R2206P02
  Default Software Version : R2206P02
  Image Name              : wa4300.ipe
```

```
Hardware Version Ver.B:
 Software Version        : R2206P02
 Default Software Version : R2206P02
 Image Name              : wa4300.ipe
Hardware Version Ver.C:
 Software Version        : R2206P02
 Default Software Version : R2206P02
 Image Name              : wa4300.ipe
Hardware Version Ver.D:
 Software Version        : R2206P02
 Default Software Version : R2206P02
 Image Name              : wa4300.ipe
Hardware Version Ver.E:
 Software Version        : R2206P02
 Default Software Version : R2206P02
 Image Name              : wa4300.ipe
Hardware Version Ver.F:
 Software Version        : R2206P02
 Default Software Version : R2206P02
 Image Name              : wa4300.ipe
```

表 1-17 コマンド出力

フィールド	説明
AP model	APモデル名
Alias	APモデル別名
Vendor name	メーカー名
Vendor ID	ベンダーID
License weight	1つのAP licenseの重みを%で使用
License type	APタイプ: ● 1:通常のAP ● 2:WTU ● 3:WT
Radio count	無線周波数
モード	サポートされている無線周波数モード
Default mode	デフォルトの無線周波数モード
BSS count	Radioで作成できる基本サービスセットの最大数
Software Version	APのソフトウェアバージョン。APによって報告されたソフトウェアバージョン番号と比較するために使用されます。デフォルトは、APDBに保存されているAPソフトウェアバージョンです。
Default Software Version	APDBに保存されているAPソフトウェアのバージョン

フィールド	説明
Image Name	APミラーファイル

関連コマンド

- wlan ap-group

1.1.24 download file

Syntax

download file *filename*

View

AP view

定義済みユーザロール

network-admin

パラメータ

filename:ファイル名。1~255 文字の文字列です。

説明

download file コマンドは、指定されたファイルを AP に送信するために使用されます。

この機能は、WLAN 高可用性ネットワーキングで CAPWAP トンネルが確立された後、マスタ AC でのみ有効です。

例

#イメージファイル main.ipe を AP ap1 にダウンロードします。

<AC> system-view

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] download file main.ipe
```

1.1.25 echo-count

Syntax

echo-count *count*

undo echo-count

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、エコー要求の送信試行の最大回数は 3 回です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

count: エコー要求の最大試行回数を 3～60 の範囲で指定します。

説明

echo-count コマンドはエコー要求の最大試行回数を設定します。

undo echo-interval コマンドはデフォルトに戻します。

AP は、指定されたエコー間隔でエコー要求を AC に送信し、CAPWAP 制御トンネルが正しく動作しているかどうかを識別します。AC は、エコー応答を送信することによって応答します。AP がキープアライブ時間内にエコー応答を受信しない場合、AP は接続を終了します。AC がキープアライブ時間内にエコー要求を受信しない場合、AC は接続を終了します。キープアライブ時間は、エコー間隔にエコー要求の最大試行回数を掛けたものです。

AP view の設定は、AP group view の設定よりも優先されます。

例

#AP が AC にエコー要求パケットを送信する最大回数を設定します。(AP view)

<AC> system-view

```
[AC] wlan ap ap3 model QX-W1110
[AC-wlan-ap-ap3] echo-count 5
```

#AP が AC にエコー要求パケットを送信する最大回数を設定します。(AP group view)

<AC> system-view

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] echo-count 5
```

1.1.26 echo-interval

Syntax

echo-interval *interval*

undo echo-interval

デフォルト

AP view は、AP group view の設定を使用します。

AP group view では、エコー要求を送信する間隔は 10 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: エコー要求の送信間隔を 5～80 秒の範囲で指定します。

説明

⚠ **注意：**

エコー間隔を 0 秒に設定すると、AP はエコー要求を送信できなくなります。この設定はテスト専用です。AC および AP 通信を正しく行うには、エコー間隔を 0 秒に設定しないでください。

AP は、指定されたエコー間隔で AC にエコー要求を送信し、CAPWAP 制御トンネルが正常に動作しているかどうかを識別します。キープアライブタイマが期限切れになる前に AP が AC からエコー応答を受信しない場合、AP は接続を終了します。キープアライブタイマが期限切れになる前に AC がエコー要求を受信しない場合、AC は接続を終了します。

キープアライブ時間は、エコー間隔に echo-count count コマンドを使用して設定されたエコー要求送信の最大試行回数を掛けたものです。計算値が 120 秒を超えると、キープアライブ時間は 120 秒に丸められます。

AP view の設定は、AP group view の設定よりも優先されます。

例

#AP が AC にエコー要求を送信する間隔を 15 秒に設定します。(AP view)

<AC> system-view

```
[AC] wlan ap ap3 model QX-W1110
[AC-wlan-ap-ap3] echo-interval 15
```

#AP が AC にエコー要求を送信する間隔を 15 秒に設定します。(AP group view)

<AC> system-view

```
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] echo-interval 15
```

1.1.27 firmware-upgrade

Syntax

firmware-upgrade { **disable** | **enable** }

undo firmware-upgrade

デフォルト

AP view:AP グループが設定されている場合は、 AP グループの設定を使用し、 AP グループが設定されていない場合は、グローバル設定を使用します。

AP group view:グローバル設定を使用します。

Global Configuration View :AP のアップグレード機能が有効になっています。

View

AP view

AP group view

Grobal configuration view

定義済みユーザロール

network-admin

説明

firmware-upgrade enable コマンドはソフトウェア更新機能を有効にします。

firmware-upgrade disable コマンドはソフトウェア更新機能を無効にします。

undo firmware-upgrade コマンドはデフォルトに戻します。

この機能により、AC は、CAPWAP トンネルの確立中に、AP のソフトウェアバージョンが AC に保存されているハードウェアバージョンおよびソフトウェアバージョンのマッピングと一致するかどうかを調べることができます。

- 一致が見つかった場合、AC は AP と CAPWAP トンネルを確立します。
- 一致するものが見つからない場合、CAPWAP トンネルの確立は次のように進行します。

a. AC は、ソフトウェアバージョンの不整合を AP に通知します。

b. 通知を受信した後、AP は AC にソフトウェアバージョンを要求し、ソフトウェアをアップグレードしてから、AC との CAPWAP トンネルを確立します。

この機能を無効にすると、AC は AP のソフトウェアバージョンを調べず、AP との CAPWAP トンネルを確立します。

AP view の設定は、AP group view の設定よりも優先されます。AP group view の設定は、global configuration view の設定よりも優先されます。

例

AP ap3 のソフトウェア更新機能を有効にします。

<AC> system-view

[AC] wlan ap ap3 model QX-W1110

[AC-wlan-ap-ap3] firmware-upgrade enable

AP group group1 の AP のソフトウェア更新機能を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] firmware-upgrade enable

#ソフトウェア更新機能をグローバルに有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] firmware-upgrade enable

関連コマンド

- wlan apdb

1.1.28 fragment-size

Syntax

fragment-size { **control** *control-size* | **data** *data-size* }

undo fragment-size { **control** | **data** }

デフォルト

AP view:AP グループ設定を使用します。

AP group view:CAPWAP 制御メッセージパケットの最大長は 1450 バイト、CAPWAP データパケットの最大長は 1500 バイトです。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

control *control-size*: CAPWAP 制御パケットの最大フラグメントサイズをバイト単位で指定します。control-size 引数の値の範囲は 1000～1450 です。

data *data-size*: CAPWAP データパケットの最大フラグメントサイズをバイト単位で指定します。control-size 引数の値の範囲は 1000～1748 です。

説明

fragment-size コマンドは CAPWAP 制御またはデータパケットの最大フラグメントサイズを設定します。

undo fragment-size コマンドは構成を削除します。

このコマンドは、AP がインターネット経由で AC に接続する場合、中間装置が AC と AP 間でパケットをドロップすることを防ぎます。

フラグメントサイズの最大変更は、オンライン AP で直ちに有効になります。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP AP1 の CAPWAP データパケットの最大フラグメントサイズを 1500 バイトに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-ap-ap1] fragment-size data 1500

AP group group1 の CAPWAP データパケットの最大フラグメントサイズを 1500 バイトに設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] fragment-size data 1500

1.1.29 gigabitethernet

🕮 **メモ**:

このコマンドのサポートは、AP モデルによって異なります。

Syntax

gigabitethernet *interface-number*

View

AP view

AP group model view

定義済みユーザロール

network-admin

パラメータ

interface-number:インタフェース番号を指定します。

説明

gigabitethernet コマンドを使用して、AP の GE Ethernet interface view に移動します。

例

AP view から GigabitEthernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1]

AP group1 の AP モデル view から GigabitEthernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] gigabitethernet 1

[AC-wlan-ap-group-group1-ap-model-QX-W1110-gigabitethernet-1]

1.1.30 hybrid-remote-ap

Syntax

hybrid-remote-ap { **disable** | **enable** }

undo hybrid-remote-ap

デフォルト

AP view:AP グループ設定を使用します。

AP group view:Remote AP 機能が無効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

説明

hybrid-remote-ap enable コマンドは、Remote AP 機能を有効にします。

hybrid-remote-ap disable コマンドは、Remote AP 機能を無効にします。

undo hybrid-remote-ap コマンドを使用して、デフォルトの状態に戻します。

デフォルトでは、AP と AC 間のトンネルが切断された場合、AP はサービスの提供を停止します。このコマンドを有効にすると、AP はリモート AP として機能し、引き続きサービスを提供できます。

このコマンドは、ローカル転送モードで動作する AP でのみ有効です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 のリモート AP を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] hybrid-remote-ap enable

AP group group1 内の AP に対してリモート AP を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] hybrid-remote-ap enable

1.1.31 if-match ip

Syntax

if-match ip *ip-address* { *mask-length* | *mask* }

undo if-match ip [*ip-address* { *mask-length* | *mask* }]

デフォルト

設定なし

View

AP group view

定義済みユーザロール

network-admin

パラメータ

ip-address: ドット付き 10 進表記で IPv4 アドレスを指定します。

mask-length: マスクの長さを 1～31 の範囲で指定します。

mask: ドット付き 10 進表記でマスクを指定します。

説明

if-match ip コマンドは IPv4 アドレスによる AP group ルールを作成します。

undo if-match ip コマンドはデフォルトに戻します。

デフォルトの AP group view ではこのコマンドを実行できません。

AP グループまたは異なる AP グループの IPv 4 アドレスによる AP グループ化ルールは、互いに重複できません。

AP グループは、IPv 4 アドレスによって最大 32 の AP グループ化ルールをサポートします。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP グループ化ルールの優先順位は降順です。グループ化ルールと一致しない AP は、デフォルトの AP グループに追加されます。

AP グループの IPv 4 アドレスと IPv 6 アドレスの両方で AP グループ化ルールを作成できます。

このコマンドの undo 形式で引数を指定しないと、IPv 4 アドレスによるすべての AP グループ化ルールが削除されます。

例

IP アドレスが 192.168.0.0/16 に属する AP を AP group group1 に追加します。

<AC> system-view

[AC] wlan ap-group group1

[AC-ap-group-group1] if-match ip 192.168.0.0 16

1.1.32 keepalive-interval

Syntax

keepalive-interval *interval*

undo keepalive-interval

デフォルト

AP view:AP グループ設定を使用します。

AP group view:AP が CAPWAP データトンネル keep alive メッセージを送信する間隔は 10 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval:AP が CAPWAP データトンネル keep alive パケットを送信する間隔。1~255 の値を秒単位で指定します。

説明

keepalive-interval コマンドはデータトンネルキープアライブ間隔を設定します。

undo keepalive-interval コマンドはデフォルトに戻します。

例

AP ap1 のデータトンネルキープアライブ間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] keepalive-interval 15

AP group 1 のデータトンネルキープアライブ間隔を 15 秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-ap-group-1] keepalive-interval 15

1.1.33 led-mode

Syntax

led-mode { **always-on** | **awake** | **normal** | **quiet** }

undo led-mode

デフォルト

AP view:AP グループ設定を使用します。

AP group view:LED 点灯モードは normal です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

always-on: always-on モードを指定します。このキーワードのサポートは、AP モデルによって異なります。

awake: awake モードを指定します。このキーワードのサポートは、AP モデルによって異なります。

normal: normal モードを指定します。このモードでの LED の点滅方法は、AP モデルによって異なります。

quiet: quiet モードを指定します。

説明

led-mode コマンドは LED 点灯モードを設定します。

undo led-mode コマンドはデフォルトに戻します。

AP group view で LED 点灯モードを awake または always-on に設定すると、指定された LED 照明モードをサポートするメンバ AP に対してのみ設定が有効になります。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 の LED 点灯モードを normal に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] led-mode normal

AP group g1 の AP に対して LED 点灯モードを awake に設定します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] led-mode awake

1.1.34 mac-address

Syntax

mac-address *mac-address*

undo mac-address *mac-address*

デフォルト

設定なし

View

AP group view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを指定します。

説明

mac-address コマンドは MAC アドレスによる AP group ルールを作成します。

undo mac-address コマンドは MAC アドレスによる AP group ルールを削除します。

このコマンドは、指定された AP が存在するかどうかを識別しません。

複数の AP group ルールを MAC アドレスで設定できます。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP group ルールの優先度は降順になっています。AP が group ルールと一致しない場合、AP はデフォルトの AP group に追加されます。

AP group ルールがすでに AP group に存在する場合、このコマンドは AP group からルールを削除します。

デフォルトの AP group の view でこのコマンドを実行することはできません。

例

AP group group1 の MAC アドレスで AP グループルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] mac-address 0AC1-F9B2-B1C2

関連コマンド

- wlan ap-group

1.1.35 mac-address

Syntax

mac-address *mac-address*

undo mac-address

デフォルト

設定なし

View

AP view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを H-H-H 形式で指定します。

説明

mac-address コマンドは AP の MAC アドレスを指定します。

undo mac-address コマンドはデフォルトに戻します。

AP が AC と CAPWAP トンネルを確立している場合、AP の MAC アドレスを変更または削除すると CAPWAP トンネルが終了します。その後、AP は AC と CAPWAP トンネルを再確立します。

例

AP ap1 の MAC アドレスを 0001-0000-0000 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] mac-address 0001-0000-0000

1.1.36 map-configuration

🕮 **メモ：**

AP の設定には **remote-configuration** を使用することを推奨します。
remote-configuration で設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。なお、**remote-configuration** を有効にした場合、**remote-configuration** で設定可能なコマンドがデフォルト値として適用されます。**remote-configuration** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

Syntax

map-configuration *filename*

undo map-configuration

デフォルト

設定なし

View

AP view

AP group's AP model view

定義済みユーザロール

network-admin

説明

filename: コンフィグレーションファイル名を指定します。コンフィグレーションファイル名は、 #を含まない 1～63 文字の文字列です。大文字と小文字を区別しません。コン

フィグレーションファイルが 本装置の記憶媒体に保管されていることを確認してください。

例

コンフィグレーション フ ァイル downconfig.txt を AP ap1 に配置します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] map-configuration downconfig.txt

コンフィグレーションファイル downconfig.txt を AP グループ apgroup1 のモデル QX-W1020 を持つ AP に配置します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] map-configuration downconfig.txt

1.1.37 port-isolate enable

🕮 **メモ：**

このコマンドのサポートは AP のモデルによって異なります。

Syntax

port-isolate { **enable** | **disable** }

undo port-isolate

デフォルト

AP の Ethernet interface view では、AP は AP グループの Ethernet interface view の設定を使用します。

AP group Ethernet interface view では、ポートアイソレーションは有効です。

AP aggregate interface view では、AP は AP グループの aggregate interface view の設定を使用します。

AP group aggregate interface view では、ポートアイソレーションは有効です。

View

AP Eth interface view

AP group Eth interface view

AP GigabitEthernet interface view

AP group GigabitEthernet interface view

AP 2.5G Ethernet interface view

AP group 2.5G Ethernet interface view

AP 10-GE interface view

AP group 10-GE interface view

AP Layer 2 aggregate interface view

AP group Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

port-isolate enable コマンドはポートアイソレーションを有効にします。

port-isolate disable コマンドはポートアイソレーションコマンドを有効にします。

undo port-isolate コマンドはデフォルトに戻します。

Ethernet interface view での設定は、そのインタフェースにのみ適用されます。

aggregate interface view での設定は、アグリゲートインタフェースとアグリゲーションメンバポートに適用されます。装置がアグリゲートインタフェースへの設定の適用に失敗した場合、装置はアイソレーショングループへの割り当てを行いません。アグリゲーションメンバポートで設定の適用に失敗した場合、装置は該当ポートをスキップし、別のアグリゲーションメンバポートをアイソレーショングループに割り当てます。

remote-configuration synchronize コマンドを使用すると、オンラインのすべての AP に設定が同期されます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 の GigabitEthernet 1 でポートアイソレーションを有効にします。

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port-isolate enable

AP グループ 1 のモデル QX-W1110 の GigabitEthernet 1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1] port-isolate enable

関連コマンド

- remote-configuration
- remote-configuration synchronize

1.1.38 port access vlan

> 🕮 **メモ：**
> このコマンドのサポートは AP のモデルによって異なります。

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

AP Ethernet interface view では、AP グループの Ethernet interface view の設定を使用します。

AP group Ethernet interface view では、AP 上のすべての access ポートが VLAN 1 に属します。

View

AP Eth Ethernet interface view

AP group Eth Ethernet interface view

AP GE Ethernet interface view

AP group GE Ethernet interface view

AP 2.5GE Ethernet interface view

AP group 2.5GE Ethernet interface view

AP XGE Ethernet interface view

AP group XGE Ethernet interface view

AP Layer 2 aggregate interface view

AP group Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: ID を 1～4094 の範囲で指定します。

説明

port access vlan コマンドは AP 上の access ポートを指定された VLAN に割り当てます。

undo port access vlan コマンドはデフォルトに戻します。

access ポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

#AP GigabitEthernet 1 ポートを VLAN 3 に追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port access vlan 3

#AP group GigabitEthernet 1 ポートを VLAN 3 に追加します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1] port access vlan 3

関連コマンド

- remote-configuration

1.1.39 port hybrid pvid

🕮 **メモ**：

このコマンドのサポートは、AP モデルによって異なります。

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

AP Ethernet interface view では、hybrid ポートは AP グループの Ethernet interface view の設定を使用します。

AP group Ethernet interface view では、hybrid ポートの PVID は、リンクタイプがアクセスされているときにポートが属する VLAN の ID です。

View

AP Eth Ethernet interface view

AP group Eth Ethernet interface view

AP GE Ethernet interface view

AP group GE Ethernet interface view

AP 2.5GE Ethernet interface view

AP group 2.5GE Ethernet interface view

AP XGE Ethernet interface view

AP group XGE Ethernet interface view

AP Layer 2 aggregate interface view

AP group Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id:インタフェースのデフォルトの VLAN ID を指定します。範囲は 1~4094 です。

説明

port hybrid pvid コマンドは AP 上の hybrid ポートの PVID を設定します。

undo port hybrid pvid コマンドは AP の hybrid ポートの PVID を 1 に設定します。

存在しない VLAN を hybrid ポートの PVID として使用できます。undo vlan コマンドを使用して hybrid ポートの PVID を削除すると、ポートの PVID 設定は変更されません。

パケットを正しく送信するには、AP の hybrid ポートと AP に接続されたスイッチの hybrid ポートに同じ PVID を設定します。

hybrid ポートが PVID からパケットを送信できるようにするには、port hybrid vlan コマンドを使用して、hybrid ポートを PVID に割り当てる必要があります。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP Ethernet interface view の設定は、AP group Ethernet interface view の設定よりも優先されます。

例

GigabitEthernet 1 を hybrid ポートとして設定し、AP ap1 の Layer 2 Ethernet interface view で PVID を VLAN 100 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-ap1-gigabitethernet-1] port hybrid pvid vlan 100

GigabitEthernet 1 を hybrid ポートとして設定し、AP グループ 1 のモデル QX-W1110 の Layer 2 Ethernet interface view で PVID を VLAN 100 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1]

port link-type hybrid

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1]

port hybrid pvid vlan 100

関連コマンド

- port hybrid vlan
- port link-type
- remote-configuration
- remote-configuration synchronize

1.1.40 port hybrid vlan

🕮 **メモ：**

このコマンドのサポートは AP のモデルによって異なります。

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

AP Ethernet interface view では、hybrid ポートは AP グループの Ethernet interface view の設定を使用します。

AP group Ethernet interface view では、hybrid ポートは、そのリンクタイプがアクセスされているときにポートが属する VLAN のタグなしメンバです。

View

AP Eth Ethernet interface view

AP group Eth Ethernet interface view

AP GE Ethernet interface view

AP group GE Ethernet interface view

AP 2.5GE Ethernet interface view

AP group 2.5GE Ethernet interface view

AP XGE Ethernet interface view

AP group XGE Ethernet interface view

AP Layer 2 aggregate interface view

AP group Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: 最大 10 個の VLAN 項目をスペースで区切って指定します。各項目は、VLAN ID または VLAN ID の範囲を vlan-id1～vlan-id2 の形式で指定します。VLAN ID の値の範囲は 1～4094 です。vlan-id2 引数の値は、vlan-id1 引数の値よりも小さくすることはできません。指定された VLAN は、装置上にすでに存在している必要があります。

tagged: 指定された VLAN のタグ付きメンバとしてポートを設定します。VLAN のタグ付きメンバは、VLAN タグを削除せずに VLAN からパケットを送信します。

untagged: ポートを、指定された VLAN のタグなしメンバとして設定します。VLAN のタグなしメンバは、VLAN タグを削除した後、VLAN からパケットを送信します。

説明

port hybrid vlan コマンドは特定の VLAN に hybrid ポートを割り当てます。

undo port hybrid vlan コマンドは指定された VLAN から hybrid ポートを削除します。

hybrid ポートは、複数の VLAN を許可できます。hybrid ポートでこのコマンドを複数回実行すると、hybrid ポートは指定されたすべての VLAN を許可します。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP Ethernet interface view の設定は、AP group Ethernet interface view の設定よりも優先されます。

例

#AP ポート GigabitEthernet 1 を hybrid ポートに設定して、VLAN 2、4、50~VLAN 100 が通過できるようにし、これらの VLAN のメッセージを送信するときに VLAN Tag を伝送します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type hybrid

[AC-wlan-ap-ap1-gigabitethernet-1] port hybrid vlan 2 4 50 to 100 tagged

#AP ポート GigabitEthernet 1 を Hybrid ポートに設定して、VLAN 2、4、50~VLAN 100 が通過できるようにし、これらの VLAN のメッセージを送信するときに VLAN Tag を伝送します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1]portlink-type hybrid

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1] port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

- port link-type
- remote-configuration
- remote-configuration synchronize

1.1.41 port link-aggregation group

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

port link-aggregation group *group-id*

undo port link-aggregation

デフォルト

AP Ethernet interface view では、AP は AP グループの Ethernet interface view の設定を使用します。

AP group Ethernet interface view では、インタフェースはアグリゲーショングループに所属していません。

View

AP Eth Ethernet interface view

AP group Eth Ethernet interface view

AP GE Ethernet interface view

AP group GE Ethernet interface view

AP 2.5GE Ethernet interface view

AP group 2.5GE Ethernet interface view

AP XGE Ethernet interface view

AP group XGE Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

group-id: アグリゲーションインタフェースの番号でアグリゲーショングループを指定します。番号の範囲は装置のモデルにより異なります。

説明

port link-aggregation group コマンドはアグリゲーショングループにインタフェースを割り当てます。

undo port link-aggregation group コマンドはアグリゲーショングループからインタフェースを除外します。

レイヤ 2 Ethernet インタフェースはレイヤ 2 アグリゲーショングループにのみ割り当てることができ、Ethernet インタフェースは 1 つのアグリゲーショングループにのみ属することができます。

アグリゲーショングループに加入すると、インタフェースはグループに設定された設定を継承します。

このコマンドを実行する前に、指定したアグリゲーショングループがすでに存在し、AP がレイヤ 2 アグリゲートインタフェースをサポートしていることを確認してください。

リモート設定同期がアクティブな場合、設定はすべてのオンライン AP に同期されます。

AP の Ethernet interface view の設定は、AP グループの Ethernet interface view の設定よりも優先されます。

例

AP ap1 の GigabitEthernet 1 をアグリゲーショングループ 1 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-aggregation group 1

AP グループ 1 のモデル QX-W1110 の GigabitEthernet 1 をアグリゲーショングループ 1 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110 gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1]

port link-aggregation group 1

関連コマンド

- remote-configuration
- remote-configuration synchronize

1.1.42 port link-type

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

AP Ethernet interface view では、イーサネットポートは AP グループの Ethernet interface view で設定を使用します。

AP group Ethernet interface view では、各イーサネットポートは access ポートです。

View

AP Eth Ethernet interface view

AP group Eth Ethernet interface view

AP GE Ethernet interface view

AP group GE Ethernet interface view

AP 2.5GE Ethernet interface view

AP group 2.5GE Ethernet interface view

AP XGE Ethernet interface view

AP group XGE Ethernet interface view

AP Layer 2 aggregate interface view

AP group Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートリンクタイプを access に設定します。

hybrid: ポートリンクタイプを hybrid に設定します。

trunk: ポートリンクタイプを trunk に設定します。

説明

port link-type コマンドは AP 上のイーサネットポートのリンクタイプを設定します。

undo port link-type コマンドはデフォルトに戻します。

この設定は、リモート設定の同期が有効になっていて、remote-configuration synchronize コマンドが設定されている場合にのみ、AP に対して同期されます。

AP Ethernet interface view の設定は、AP Ethernet interface view の設定よりも優先されます。

例

AP ap1 の Layer 2 Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type trunk

AP グループ 1 のモデル QX-W1110 の AP の Layer 2 Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1] port link-type trunk

関連コマンド

remote-configuration

1.1.43 port trunk permit vlan

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

AP Ethernet interface view では、trunk ポートは AP グループの Ethernet interface view の設定を使用します。

AP group Ethernet interface view では、trunk ポートは VLAN 1 からのパケットだけを通過させます。

View

AP Eth Ethernet interface view

AP group Eth Ethernet interface view

AP GE Ethernet interface view

AP group GE Ethernet interface view

AP 2.5GE Ethernet interface view

AP group 2.5GE Ethernet interface view

AP XGE Ethernet interface view

AP group XGE Ethernet interface view

AP Layer 2 aggregate interface view

AP group Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: 最大 10 個の VLAN 項目をスペースで区切って指定します。各項目は、VLAN ID または VLAN ID の範囲を vlan-id1～vlan-id2 の形式で指定します。VLAN ID の値の範囲は 1～4094 です。vlan-id2 引数の値は、vlan-id1 引数の値よりも小さくすることはできません。

all: すべての VLAN を指定します。

説明

port trunk permit vlan コマンドは指定された VLAN に trunk ポートを割り当てます。

undo port trunk permit vlan コマンドは指定された VLAN から trunk ポートを削除します。

trunk ポートは、複数の VLAN を許可できます。このコマンドを trunk ポート上で複数回実行すると、trunk ポートは指定されたすべての VLAN を許可します。

trunk ポートでは、PVID からのパケットだけがタグなしを通過できます。

許可されていない VLAN ユーザがポートを介して制限されたリソースにアクセスするのを防ぐには、port trunk permit vlan all コマンドを慎重に使用してください。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP Ethernet interface view の設定は、AP Ethernet interface view の設定よりも優先されます。

例

GigabitEthernet 1 を trunk ポートとして設定し、AP ap1 の Layer 2 Ethernet interface view で VLAN 100、VLAN 2、VLAN 4 を介して VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-ap1-gigabitethernet-1] port trunk permit vlan 2 4 50 to 100

GigabitEthernet 1 を trunk ポートとして設定し、AP グループ 1 のモデル QX-W1020 の AP の Ethernet interface view で VLAN 100、VLAN 2、VLAN 4 を介して VLAN 50 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1] port trunk permit vlan 2 4 50 to 100

関連コマンド

- port link-type
- remote-configuration
- remote-configuration synchronize

1.1.44 port trunk pvid

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

AP Ethernet interface view では、trunk ポートは AP グループの Ethernet interface view の設定を使用します。

AP Ethernet interface view では、trunk ポートの PVID は VLAN 1 です。

View

AP Eth Ethernet interface view

AP group Eth Ethernet interface view

AP GE Ethernet interface view

AP group GE Ethernet interface view

AP 2.5GE Ethernet interface view

AP group 2.5GE Ethernet interface view

AP XGE Ethernet interface view

AP group XGE Ethernet interface view

AP Layer 2 aggregate interface view

AP group Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: ID を 1～4094 の範囲で指定します。

説明

port trunk pvid コマンドは AP 上の trunk ポートの PVID を設定します。

undo port trunk pvid コマンドはデフォルトに戻します。

存在しない VLAN を trunk ポートの PVID として使用できます。undo vlan コマンドを使用して trunk ポートの PVID を削除すると、ポートの PVID 設定は変更されません。

パケットを正しく送信するには、AP の hybrid ポートと AP に接続されたスイッチの hybrid ポートに同じ PVID を設定します。

trunk ポートが PVID からパケットを送信できるようにするには、port trunk permit vlan コマンドを使用して、trunk ポートを PVID に割り当てる必要があります。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP Ethernet interface view の設定は、AP group Ethernet interface view の設定よりも優先されます。

例

AP ap1 の Layer 2 Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定し、PVID を VLAN 100 に設定し、VLAN 100 に割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] gigabitethernet 1

[AC-wlan-ap-ap1-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-ap1-gigabitethernet-1] port trunk pvid vlan 100

[AC-wlan-ap-ap1-gigabitethernet-1] port trunk permit vlan 100

AP グループの Ethernet interface view で、GigabitEthernet 1 を trunk ポートとして設定し、PVID を VLAN 100 に設定し、VLAN 100 に割り当てます。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] gigabitethernet 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1] port link-type trunk

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1] port trunk pvid vlan 100

[AC-wlan-ap-group-1-ap-model-QX-W1110-gigabitethernet-1] port trunk permit vlan 100

関連コマンド

- port link-type
- port trunk permit vlan
- remote-configuration
- remote-configuration synchronize

1.1.45 power-level default

🕮 **メモ：**

- **power-level default** コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。
- QX-W1210 と QX-W1230 はデフォルトの給電モード(High)の設定で 25W 以下の消費電力で動作します。

Syntax

power-level default

undo power-level default

デフォルト

AP view では、AP は AP group の AP model view の設定を使用します。

AP group の AP model view では AP の給電モードは High です。

View

AP view（QX-W1200 シリーズのみ）

AP group view（QX-W1200 シリーズのみ）

定義済みユーザロール

network-admin

パラメータ

high: 10G Ethernet インタフェースの最大リンク速度、USB インタフェース利用を制限しません。

middle: 10G Ethernet インタフェースの最大リンク速度を 5Gbps に制限し、USB インタフェースを使用不可にします。

low: 10G Ethernet インタフェースの最大リンク速度を 2.5Gbps に制限し、USB インタフェースを使用不可にします。

説明

power-level default コマンドは、AP の給電モードを指定します。

undo power-level default コマンドはデフォルトに戻します。

10G Ethernetインタフェースの最大リンク速度とUSBインタフェースの利用を制限することにより、消費電力を 25W 以下に制限し PoE+(802.3at)給電での動作を可能にします。

- PoE++(802.3bt)もしくは AC アダプタによる給電の場合は、**high** を設定します
- PoE+(802.3at)による給電の場合は、**middle** または **low** を設定します。

表 1-18 に AP の給電モード設定時の動作仕様を示します。

表 1-18 AP の給電モードの動作仕様

動作仕様 / AP の給電モード	装置の消費電力制限	10G Ethernet インタフェース最大リンク速度	USB インタフェース利用制限
high	制限なし	制限なし	制限なし (QX-W1230 は使用不可)
middle	25W	5Gbps	使用不可
low	25W	2.5Gbps	使用不可

🕮 **メモ：**

- 10G Ethernet インタフェースの通信速度が ”10000” または ”5000” の固定設定の場合、AP の給電モード設定 “low” を設定することはできません。
- 10G Ethernet インタフェースの通信速度が ”10000” の固定設定の場合、AP の給電モード設定 “middle” と “low” を設定することはできません。
- AP の給電モード設定 ”middle” または ”low” が設定されている場合、10G Ethernet インタフェースの通信速度、通信モードを変更することはできません。
- AP の給電モード設定による USB インタフェースの利用制限は ”usb enable” コマンドの設定よりも優先されます。
- AP の給電モードを異なるモードに変更する場合、AutoNegotiation をやり直すため 10G Ethernet インタフェースがリンクダウンします。

例

AP **ap1**（QX-W1240）の給電モードを **middle** に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] power-level default middle

AP グループ 1 のモデル **QX-W1240** の AP の給電モードを **low** に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1240

[AC-wlan-ap-group-1-ap-model-QX-W1240] power-level default low

関連コマンド

usb

1.1.46 priority

Syntax

priority *priority*

undo priority

デフォルト

AP view:AP group 設定を使用します。

AP group view:AP の接続優先順位は 4 です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

priority:AP 接続の優先度。範囲は 0~7 です。この値が大きいほど、優先順位が高くなります。

説明

priority コマンドは AC の AP 接続優先度を設定します。

undo priority コマンドはデフォルトに戻します。

AP は、より高い接続優先度を有する AC と CAPWAP トンネルを優先して確立します。

AP 接続優先度は、AC ディスカバリ中にのみ有効です。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap3 の AP 接続優先度を 7 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1110

[AC-wlan-ap-ap3] priority 7

AP group group1 の、AP 接続優先度を 7 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] priority 7

1.1.47 region-code

Syntax

region-code JP

デフォルト

JP

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

地域コードは、使用可能な周波数、利用可能なチャネル、および送信電力レベルなどの特性を決定します。 AP を設定する前に有効な地域コードを設定してください。

AP view、 AP group view 、および Global configuration view での設定の優先順位は降順です。

例

global の地域コードを JP に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] region-code JP

1.1.48 region-code-lock

Syntax

region-code-lock { disable | enable }

undo region-code-lock

デフォルト

AP view: AP group view の設定を継承します。

AP group view: global configuration view の設定を継承します。

Global configuration view: ロックしません。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: 地域コードのロックを解除します。

enable: 地域コードをロックします。

説明

region-code lock enable コマンドは地域コードをロックします。

region-code lock disable コマンドは地域コードのロックを解除します。

undo region code lock コマンドはデフォルトに戻します。

ロックされたリージョンコードは変更できません。

AP view に地域コードを設定していない場合、 AP view で地域コードをロックしても、AP は AP group view または AP group view に設定された地域コードを使用します。AP group view に地域コードが設定していない場合、 AP group view で地域コードをロックしても、AP はグローバル地域コードを使用します。

AP view、 AP group view 、および Global configuration view での設定の優先順位は降順です。

例

AP ap1 の地域コードをロックします。

<AC> system-view

[AC] wlan ap ap1 model WA6320

[AC-wlan-ap-ap1] region-code-lock enable

AP group group1 の地域コードをロックします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] region-code-lock enable

global の 地域コードをロックします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] region-code-lock enable

例

- **region-code**

1.1.49 remote-configuration

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

remote-configuration { **disable** | **enable** }

undo remote-configuration enable

デフォルト

AP view:AP グループ設定を継承します。

AP group view:リモート構成の同期が無効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable: リモート構成割り当て機能を無効にします。

enable: リモート構成割り当て機能を有効にします。

説明

remote-configuration enable コマンドはリモート構成割り当て機能を有効にします。

remote-configuration disable コマンドはリモート構成割り当て機能を無効にします。

undo remote-configuration コマンドはデフォルトに戻します。

AC は、リモート設定割り当て機能が有効になっている場合にのみ、関連する VLAN 設定を AP に割り当てます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 のリモート設定割り当て機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] remote-configuration enable

APgroup group1 のリモート設定割り当て機能を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] remote-configuration enable

1.1.50 remote-configuration synchronize

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

remote-configuration synchronize

デフォルト

AP view では、AP は AP group view の設定を使用します。

AP group view では、リモート設定同期は起動していません。

View

AP view

AP group view

定義済みユーザロール

network-admin

説明

⚠ **注意：**

このコマンドは、オンライン AP 上のすべての VLAN、リンクアグリゲーション、およびポートの設定(ポートアイソレートを除く)を削除し、AC 上の設定を AP に反映させるコマンドです。注意して使用してください。これらの設定が削除できない場合、AC 上で設定の競合している可能性があります。AC での設定を確認してください。

remote-configuration synchronize コマンドは AC の設定を AP に同期します。

AP のコンフィグレーションファイルを更新するには、map-configuration コマンドを使用してコンフィグレーションファイルを AP に展開することができます。しかし、コンフィグレーションファイルを AP に展開する前に、そのファイルにコマンドを記述しておく必要があります。この方法は、時間がかかるため、AP が数多く存在するネットワークでは適用できません。

本機能により、AC は VLAN、リンクアグリゲーション、ポートアイソレーションといった設定を、オンラインの AP に対して直接同期させることができます。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 に対してリモートコンフィグレーションシンクロナイゼーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] remote-configuration synchronize

AP グループ group1 の AP に対してリモートコンフィグレーションシンクロナイゼーションを有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] remote-configuration synchronize

関連コマンド

- remote-configuration

1.1.51 reset wlan ap

Syntax

reset wlan ap { **all** | **ap-group** *group-name* | **model** *model-name* | **name** *ap-name* | **native** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: AC に接続されているすべての AP を指定します。

name *ap-name*: AP を名前で指定します。大文字と小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

model *model-name*: モデル名で AP モデルを指定します。

ap-group *group-name*: AP group を名前で指定します。大文字と小文字を区別しない 1～31 文字です。

native:AC と CAPWAP トンネルを確立したすべての AP を指定します。

説明

reset wlan ap コマンドを使用して AP をリセットします。

このコマンドは、AP と AC 間の CAPWAP トンネルを終了し、AP に関するすべての接続情報を削除します。

例

AP ap1 をリセットします。

<AC> reset wlan ap name ap1

```
Resetting the APs will terminate the CAPWAP tunnels with the AC.Continue?[Y/N]:
```

1.1.52 reset wlan ap connection-record

Syntax

reset wlan ap { **all** | **name** *ap-name* } **connection-record**

View

User view

定義済みユーザロール

network-admin

パラメータ

all：すべての AP の接続記録をクリアします。

name *ap-name*：AP の名前を 1 ～ 64 文字の文字列で指定します。これには、文字、数字、アンダースコア、「.」、「[」、「]」、「/」、「-」、サイズを含めることができます-センシティブな書き込み

説明

reset wlan ap connection-record コマンドを使用して、AC の AP 接続レコードを削除します。

例

AC 上のすべての AP 接続レコードを削除します。

<AC> reset wlan ap all connection-record

1.1.53 reset wlan ap reboot-log

Syntax

reset wlan ap reboot-log { **all** | **name** *ap-name*}

View

User view

定義済みユーザロール

network-admin

パラメータ

all：すべての AP の再起動ログ情報を削除します。

name *ap-name*：指定した AP の再起動ログ情報を削除します。 *ap-name* は 1 ～ 64 文字の文字列で、文字、数字、アンダースコア、「.」、「[」、「]」、「/」 および「-」、大文字と小文字が区別されます。

説明

reset wlan ap reboot-log コマンドを使用して、指定した AP またはすべての AP の再起動ログ情報を削除します。

例

ap1 の再起動ログ情報を削除します。

<AC> reset wlan ap reboot-log name ap1

関連コマンド

- display wlan ap reboot-log

1.1.54 reset wlan ap statistics association-failure-record

🕮 **メモ**：

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでサポートしています。

Syntax

reset wlan ap statistics association-failure-record

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

reset wlan ap statistics association-failure-record コマンドを使用して、AP 関連付け失敗理由の統計情報を削除します。

例

AP 関連付け失敗理由の統計情報を削除します。

<AC> reset wlan ap statistics association-failure-record

1.1.55 reset wlan ap statistics image-download

🕮 **メモ**:

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでサポートしています。

Syntax

reset wlan ap statistics image-download { **all** | **failed** | **in-progress** | **succeeded** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all：すべての AP の AP イメージダウンロード統計情報を削除します。

failed：失敗した AP イメージダウンロードの統計情報を削除します。

in-progress：進行中の AP イメージダウンロードの統計情報を削除します。

succeeded：成功した AP イメージダウンロードの統計情報を削除します。

説明

reset wlan ap statistics association-failure-record コマンドを使用して、AP イメージのダウンロード統計情報を削除します。

例

成功した AP イメージダウンロードの統計情報を削除します。

<AC> reset wlan ap statistics association-failure-record succeeded

失敗した AP イメージダウンロードの統計情報を削除します。

<AC> reset wlan ap statistics association-failure-record failed

進行中の AP イメージダウンロードの統計情報を削除します。

<AC> reset wlan ap statistics association-failure-record in-progress

1.1.56 reset wlan ap statistics online-record

🕮 メモ：

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでサポートしています。

Syntax

reset wlan ap statistics online-record

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

reset wlan ap statistics online-record コマンドを使用して、オンラインの AP 数量の統計情報を削除します。

例

オンラインの AP 数量の統計情報を削除します。

<AC> reset wlan ap statistics online-record

1.1.57 reset wlan ap statistics tunnel-down-record

🕮 メモ：

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでサポートしています。

Syntax

reset wlan ap statistics tunnel-down-record

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

reset wlan ap statistics tunnel-down-record コマンドを使用して、AC と AP の CAPWAP トンネル接続断の統計情報を削除します。

例

AC と AP の CAPWAP トンネル接続断の統計情報を削除します。

<AC> reset wlan ap statistics tunnel-down-record

1.1.58 reset wlan ap statistics switch-over-record

🕮 **メモ**:

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでサポートしています。

Syntax

reset wlan ap statistics switch-over-record

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

reset wlan ap statistics switch-over-record コマンドを使用して、マスタとスタンバイのリンクの切り替えの統計情報を削除します。

例

マスタとスタンバイのリンクの切り替えの統計情報を削除します。

<AC> reset wlan ap statistics switch-over-record

1.1.59 retransmit-count

Syntax

retransmit-count *value*

undo retransmit-count

デフォルト

AP view:AP グループ設定を継承します。

AP group view:要求パケットの再送信回数は 3 回です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

value: AC 要求再送信の最大試行回数を 2～5 の範囲で指定します。

説明

retransmit-count コマンドは AC 要求の再送信の最大試行回数を設定します。

undo retransmit-count コマンドはデフォルトに戻します。

AC は、要求再送の最大試行回数に達するか応答が受信されるまで、再送信間隔で AP に送信された要求を送信します。

AC から AP に送信される要求には、次のタイプがあります。

- イメージデータ要求
- 設定更新要求
- リセット要求
- データ転送要求
- IEEE 802.11 WLAN 設定要求
- ステーション設定要求

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap3 の AC 要求の再送信の最大試行回数を 4 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1110

[AC-wlan-ap-ap3] retransmit-count 4

AP group group1 の AP の AC 要求再送信の最大試行数を 4 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] retransmit-count 4

関連コマンド

- retransmit-interval

1.1.60 retransmit-interval

Syntax

retransmit-interval *interval*

undo retransmit-interval

デフォルト

AP view:AP グループ設定を使用します。

AP group view:要求パケットの再送信間隔は 5 秒です。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

interval: 要求の再送信間隔を 3～8 秒の範囲で指定します。

説明

retransmit-interval コマンドは AC が AP への要求を再送信する間隔を設定します。

undo retransmit-interval コマンドはデフォルトに戻します。

AC から AP に送信される要求には、次のタイプがあります。

- イメージデータ要求
- 設定更新要求
- リセット要求
- データ転送要求
- IEEE 802.11 WLAN 設定要求
- ステーション設定要求

AP view の設定は、AP group view の設定よりも優先されます。

例

AC が AP ap3 に要求を送信する際の、要求の再送信間隔を 6 秒に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1110

[AC-wlan-ap-ap3] retransmit-interval 6

AC が AP group group1 内の AP に要求を送信する際の、要求の再送信間隔を 6 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] retransmit-interval 6

関連コマンド

- retransmit-count

1.1.61 serial-id

Syntax

serial-id *serial-id*

undo serial-id *serial-id*

デフォルト

設定なし

View

AP group view

定義済みユーザロール

network-admin

パラメータ

serial-id: AP のシリアル ID を、大文字と小文字を区別しない 1～63 文字で指定します。

説明

serial-id コマンドはシリアル ID で AP group ルールを作成します。

undo serial-id コマンドはシリアル ID で AP group ルールを削除します。

このコマンドは、指定された AP が存在するかどうかを識別しません。

シリアル ID で複数の AP group ルールを設定できます。

AP 名、シリアル ID、MAC アドレス、IP アドレスによる AP group ルールの優先度は、降順になっています。AP が group ルールと一致しない場合、AP はデフォルトの AP group に追加されます。

AP group ルールがすでに AP group に存在する場合、このコマンドは AP group からルールを削除します。

デフォルトの AP group view でこのコマンドを実行することはできません。

例

AP group group1 のシリアル ID で AP group ルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] serial-id 210235A1BSC123000037

関連コマンド

- wlan ap-group

1.1.62 serial-id

Syntax

serial-id *serial-id*

undo serial-id

デフォルト

設定なし

View

AP view

定義済みユーザロール

network-admin

パラメータ

serial-id: AP のシリアル ID を、大文字と小文字を区別しない 1～63 文字で指定します。

説明

serial-id コマンドは AP のシリアル ID を指定します。

undo serial-id コマンドはデフォルトに戻します。

AP が AC との CAPWAP トンネルを確立している際に、AP のシリアル ID を変更または削除すると、CAPWAP トンネルが終了します。その後、AP は AC と CAPWAP トンネルを再確立します。

例

AP ap1 のシリアル ID を 219801 A28N819CE0002T に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-ap-ap1] serial-id 219801A28N819CE0002T

1.1.63 smartrate-ethernet

🕮 **メモ**:

このコマンドのサポートは、AP モデルによって異なります。

Syntax

smartrate-ethernet *interface-number*

View

AP view

AP group AP model view

定義済みユーザロール

network-admin

パラメータ

interface-number: インタフェース番号を指定します。値の範囲は、AP モデルによって異なります。

説明

smartrate-ethernet コマンドは AP の 2.5 GigabitEthernet interface view に移行します。

例

AP view から Smartrate-Ethernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1120

[AC-wlan-ap-ap1] smartrate-ethernet 1

[AC-wlan-ap-ap1-smartrate-ethernet-1]

AP group group1 の AP model view から Smartrate-Ethernet 1 の interface view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1120

[AC-wlan-ap-group-group1-ap-model-QX-W1120] smartrate-ethernet 1

[AC-wlan-ap-group-group1-ap-model-QX-W1120-smartrate-ethernet-1]

1.1.64 snmp-agent trap enable wlan ap

Syntax

snmp-agent trap enable wlan capwap

undo snmp-agent trap enable wlan capwap

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan ap コマンドは AP 管理の SNMP 通知を有効にします。

undo snmp-agent trap enable wlan ap コマンドはデフォルトに戻します。

重要な AP 管理イベントを NMS に報告するには、AP 管理の SNMP 通知を有効にします。生成されたトラップ情報は、デバイスの SNMP モジュールに送信されます SNMP でトラップ情報の送信パラメータを設定することにより、トラップ情報出力の関連する属性が決定されます。トラップ情報の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

例

AP 管理の SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan ap

1.1.65 snmp-agent trap enable wlan capwap

Syntax

snmp-agent trap enable wlan capwap

undo snmp-agent trap enable wlan capwap

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan capwap コマンドは CAPWAP の SNMP 通知を有効にします。

undo snmp-agent trap enable wlan capwap コマンドはデフォルトに戻します。

重要な CAPWAP イベントを NMS に報告するには、CAPWAP の SNMP 通知を有効にします。生成されたトラップ情報は、デバイスの SNMP モジュールに送信されます SNMP でトラップ情報の送信パラメータを設定することにより、トラップ情報出力の関連する属性が決定されます。トラップ情報の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

例

CAPWAP の SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan capwap

1.1.66 statistics-interval

Syntax

statistics-interval *interval*

undo statistics-interval

デフォルト

AP view:AP グループが設定されている場合、AP group の設定を使用します。AP group が設定されていない場合、grobal 設定が継承されます。

AP group view: grobal 設定を使用します。

Grobal configuration view:AP が AC に Radio 統計情報を報告する間隔は 50 秒です。

View

AP view

AP group view

Grobal configuration view

定義済みユーザロール

network-admin

パラメータ

interval: 統計値報告間隔を 0～240 秒の範囲で指定します。AP の統計値報告を無効にするには、統計値報告間隔を 0 に設定します。

説明

statistics-interval コマンドは AP が統計値報告を AC に送信する間隔を設定します。

undo statistics-interval コマンドはデフォルトに戻します。

このコマンドを実行すると、AP が統計情報を報告する間隔を変更できます。これらの統計情報を使用して、AP 上の無線の動作ステータスを監視できます。

AP view、AP group view、Global configuration view の順に優先されます。

例

AP ap1 の統計値報告間隔を 10 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] statistics-interval 10

AP group group1 の AP の統計値報告間隔を 10 秒に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] statistics-interval 10

#AP の Radio 統計情報報告間隔を 10 秒に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] statistics-interval 10

1.1.67 ten-gigabitethernet

🕮 **メモ**:

このコマンドのサポートは、AP モデルによって異なります。

Syntax

ten-gigabitethernet *interface-number*

View

AP view

AP group ap-model view

定義済みユーザロール

network-admin

パラメータ

interface-number:インタフェース番号を指定します。

説明

ten-gigabitethernet コマンドを使用して、AP の Ten-GigabitEthernet view に移行します。

例

#AP の Ten-GigabitEthernet 1 view に移行します。（AP view）

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] ten-gigabitethernet 1

[AC-wlan-ap-ap1-ten-gigabitethernet-1]

#AP の Ten-GigabitEthernet 1 view に移行します。（AP group ap-model view）

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] ten-gigabitethernet 1

[AC-wlan-ap-group-group1-ap-model-QX-W1110-ten-gigabitethernet-1]

1.1.68 tunnel encryption

Syntax

tunnel encryption { **disable** | **enable** }

undo tunnel encryption

デフォルト

AP view:AP group 設定を使用します。

AP group view:CAPWAP 制御トンネル暗号化機能が無効になっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

disable:CAPWAP トンネル暗号化機能を無効にします。

enable:CAPWAP トンネル暗号化機能を有効にします。

説明

tunnel encryption enable コマンドは、CAPWAP 制御トンネル暗号化機能を有効にします。

tunnel encryption disable コマンドは、CAPWAP 制御トンネル暗号化機能を無効にします。

undo tunnel encryption コマンドを使用はデフォルトに戻します。

この機能を有効にすると、AP は AC に再接続されます。

CAPWAP 制御トンネル暗号化機能が有効になった後、AC から AP に送信される Discovery Response パケットには暗号化フラグが含まれます. Discovery Response パケットを受信した AP は、AC と DTLS ハンドシェイクを実行し、AC の確立を完了します。AP と AC が DTLS ハンドシェイクを完了した後に交換される CAPWAP コントロールトンネルパケットは、暗号化されて送信されます。

AP view での設定は、AP group view での設定よりも優先されます。

例

#AP の CAPWAP 制御トンネル暗号化機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] tunnel encryption enable

This operation will reconnect the AP.Continue?[Y/N]

#AP group の CAPWAP 制御トンネル暗号化機能を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] tunnel encryption enable

```
This operation will reconnect member APs that are not enabled with CAPWAP control
tunnel encryption.Continue?[Y/N]
```

1.1.69 vlan

🕮 メモ：

このコマンドのサポートは、AP モデルによって異なります。

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] }

undo vlan { *vlan-id1* [**to** *vlan-id2*] }

デフォルト

AP view:AP group の設定を使用します。

AP group view:VLAN1 が存在します。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

vlan-id1: VLAN ID を 1～4094 の範囲で指定します。

vlan-id1 to vlan-id2: VLAN 範囲を指定します。vlan-id1 および vlan-id2 引数は VLAN ID を指定します。2 つの引数の値の範囲は 1～4094 です。vlan-id2 引数の値は、vlan-id1 引数の値よりも小さくすることはできません。

説明

vlan vlan-id コマンドは AP の VLAN を作成し、AP の VLAN view に移行します。

vlan vlan-id1 to vlan-id2 は、AP の VLAN vlan-id1～vlan-id2 を作成します。

undo vlan コマンドは AP の指定された VLAN を削除します。

VLAN 1（デフォルト VLAN）または予約済み VLAN を作成または削除することはできません。

このコマンドを AP で有効にするには、リモート設定割り当て機能が有効になっていることを確認してください。

AP view の設定は、AP group view の設定よりも優先されます。

例

AP ap1 の VLAN 2 を作成し、VLAN の VLAN view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] vlan 2

[AC-wlan-ap-ap1-vlan2]

APgroup group1 の VLAN 2 を作成し、VLAN の VLAN view に移行します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] vlan 2

[AC-wlan-ap-group-1-vlan2]

関連コマンド

- remote-configuration
- remote-configuration synchronize

1.1.70 wlan ap

Syntax

wlan ap *ap-name* [**model** *model-name*]

undo wlan ap *ap-name*

デフォルト

手動 AP は存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ap-name: AP を名前で指定します。大文字と小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を使用できます。

model *model-name*: AP のモデル名を指定します。AP を作成するときは、モデル名を指定する必要があります。

説明

wlan ap コマンドは AP を作成し AP view へ移行します。

undo wlan ap コマンドは AP を削除します。

指定された AP がすでに存在する場合、AP view に入ります。

指定された AP が CAPWAP トンネルを確立している場合、undo wlan ap コマンドはトンネルも終了します。

例

#ap 1 を作成します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1]

1.1.71 wlan apdb

Syntax

wlan apdb *model-name hardware-version software-version*

undo wlan apdb *model-name hardware-version*

デフォルト

AP モデルのハードウェアバージョンに対するソフトウェアバージョンは、APDB ユーザスクリプト内に記憶されているソフトウェアバージョンです。

View

System view

定義済みユーザロール

network-admin

パラメータ

model-name: APDB の AP モデル名を指定します。

hardware-version: APDB のハードウェアバージョンを指定します。

software-version: AP ソフトウェアバージョンを大文字と小文字を区別しない 1～31 文字で指定します。

説明

⚠ **注意：**

CAPWAP トンネル確立の失敗を回避するには、NEC サポートの指示に従ってこのコマンドを使用します。

wlan apdb コマンドは AP モデルのソフトウェアバージョンとハードウェアバージョン間のマッピングを設定します。

undo wlan apdb コマンドはデフォルトに戻します。

このコマンドは、ソフトウェアのアップグレード時にソフトウェアバージョンの整合性チェックを行うために、ソフトウェアのアップグレード機能とともに使用されます。

このコマンドは、AP に必要なソフトウェアバージョンが、APDB に格納されている AP モデルに指定されているソフトウェアバージョンと一致しない場合にのみ使用します。

例

#AP モデル QX-W1110 ハードウェアバージョン Ver.C 対応するソフトウェアバージョンは E2108 です。

<AC> system-view

[AC] wlan apdb QX-W1110 Ver.C E2108

関連コマンド

- firmware-upgrade

1.1.72 wlan apdb file

Syntax

wlan apdb file *user.apdb*

undo wlan apdb file

デフォルト

APDB ユーザスクリプトはロードされません。

View

System view

定義済みユーザロール

network-admin

パラメータ

user.apdb: APDB ユーザプロファイルを名前で指定します。大文字と小文字が区別される 1～63 文字です。apdb はファイル名の拡張子です。

説明

wlan apdb file は、APDB ユーザスクリプトをロードします。

undo wlan apdb file は APDB ユーザスクリプトを削除します。

APDB ユーザスクリプトをロードする場合は、次の制限とガイドラインに従ってください。

- AC で複数のユーザスクリプトをロードすると、最後にロードされたユーザスクリプトによって古いユーザスクリプトが上書きされます。

- ユーザスクリプトが有効であることを確認します。無効なスクリプトはロード失敗の原因となります。
- ユーザスクリプト内の AP モデルは、システムスクリプト内の AP モデルとは異なる必要があります。
- ファイルシステムでユーザスクリプトの名前を変更する場合は、ユーザスクリプトをリロードして、ユーザスクリプトの AP モデル設定が AC リブート後に失われないようにします。
- ファイルシステムでユーザ文字を新しいユーザ文字に置き換える場合は、新しいユーザ文字をリロードします。新しいユーザスクリプトに、置き換えられたユーザスクリプトに保存された AP モデル情報が含まれていない場合、AC 再起動後に AP モデル情報は失われます。
- ファイルシステムでユーザスクリプトを削除した場合は、新しいユーザスクリプトをリロードします。新しいユーザスクリプトをリロードしない場合、ユーザスクリプト内の AP モデル設定は AC リブート後に失われます。

古いユーザスクリプトがすでに存在する場合は、APDB ユーザスクリプトをロードするときに次の制限とガイドラインに従ってください。

- 古いユーザスクリプトにモデルが記載されている手動 AP またはオンライン自動 AP が存在する場合、AC 上の対応する AP モデル情報を削除するときにのみ、新しいユーザスクリプトをロードできます。
- 古いユーザスクリプトに記載されている AP モデルの AP が AP グループに追加されている場合、AP グループから AP を削除するときにのみ、新しいユーザスクリプトをロードできます。
- 古いユーザスクリプトにソフトウェアバージョンがすでに設定されている AP モデルが含まれている場合、wlan apdb コマンドを使用して元のソフトウェアバージョンを復元するときにのみ、新しいユーザスクリプトをロードできます。

例

#ユーザスクリプト user.apdb をロードします。

<AC> system-view

[AC] wlan apdb file user.apdb

関連コマンド

- wlan apdb

1.1.73 wlan ap-group

Syntax

wlan ap-group *group-name*

undo wlan ap-group *group-name*

デフォルト

デフォルトの AP group default-group が存在します。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name: AP group を名前で指定します。大文字と小文字を区別しない 1～31 文字です。

説明

wlan ap-group コマンドは AP group を作成します。

undo wlan ap-group コマンドは AP group を削除します。

指定された AP group が存在する場合、AP group view に移行します。

デフォルトの AP group は削除できません。

例

group1 という名前の AP group を作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1]

関連コマンド

- display wlan ap-group

1.1.74 wlan ap-image-deploy

Syntax

wlan ap-image-deploy { all | ap-group *group-name* **| name** *ap-name* **}**

View

System view

定義済みユーザロール

network-admin

パラメータ

all:すべての AP を指定します。

ap-group *group-name*:AP グループを名前で指定します。1 から 31 文字の文字列で、大文字と小文字は区別されません。指定した AP グループがすでに存在している必要があります。

name *ap-name*:AP を名前で指定します。1 から 64 文字の文字列で、大文字と小文字が区別されます。文字列には、文字、数字、アンダースコア(_)、ドット（。）、左かっこ（[）、右括弧(])）、スラッシュ(/)、およびハイフン(-)を含めることができます。指定した AP はすでに存在している必要があります。

説明

wlan ap-image-deploy を使用して、すべてのオンライン AP にイメージファイルを展開します。アップグレードを有効にするには、アップグレード後に AP を再起動します。

このコマンドを実行する前に、イメージファイルを AC のストレージメディアにアップロードする必要があります。**wlan image-load filepath** コマンドを実行して、記憶媒体を指定できます。

例

#すべてのオンライン状態の AP にイメージファイルを展開します。

<AC> system-view

[AC] wlan ap-image-deploy all

関連コマンド

- wlan image-load filepath

1.1.75 wlan auto-ap enable

Syntax

wlan auto-ap enable

undo wlan auto-ap enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan auto-ap enable コマンドは自動 AP 機能を有効にします。

undo wlan auto-ap enable コマンドは自動 AP 機能を無効にします。

自動 AP 機能により、AP は手動 AP 設定なしで AC に接続可能となります。数多くの AP を WLAN 内に配置する際の設定が単純化されます。

自動 AP を設定するために、自動 AP を手動 AP に変換するための自動 AP パーシステンスを使用するか、もしくは AP group を通じてそれを設定しなければなりません。

例

#自動 AP 機能を有効にします。

<AC> system-view

[AC] wlan auto-ap enable

1.1.76 wlan auto-ap persistent

Syntax

wlan auto-ap persistent { **all** | **name** *auto-ap-name* [*new-ap-name*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

all: すべてのオンライン自動 AP を指定します。このキーワードを指定すると、コマンドはすべてのオンライン自動 AP を名前が変更されていない手動 AP に変換します。

name *auto-ap-name*: オンライン自動 AP を指定します。

new-ap-name: AP の新しい名前を指定します。大文字と小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を使用できます。この引数を指定しない場合、変換された手動 AP は自動 AP の名前を使用します。

説明

wlan auto-ap persistent コマンドはオンライン自動 AP を手動 AP に変換します。

例

MAC アドレスが 0afb-4212-cd36 の自動 AP を手動 AP ap2 に変換します。

<AC> system-view

[AC] wlan auto-ap persistent name 0001-ab12-cd36 ap2

1.1.77 wlan auto-persistent enable

Syntax

wlan auto-persistent enable

undo wlan auto-persistent enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan auto-persistent enable コマンドは自動 AP パーシステンスを有効しオンラインになった後に自動 AP を自動的に手動 AP に変換します。

undo wlan auto-persistent enable コマンドはデフォルトに戻します。

このコマンドは、コマンドを実行した後にオンラインになった自動 AP でのみ有効です。すでにオンラインになっている自動 AP の場合は、**wlan auto-ap persistent** コマンドを使用して、手動 AP に変換します。

例

#自動 AP パーシステンスを有効にします。

<AC> system-view

[AC] wlan auto-persistent enable

1.1.78 wlan capwap discovery-policy unicast

Syntax

wlan capwap discovery-policy unicast

undo wlan capwap discovery-policy

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan capwap discovery-policy unicast コマンドは AC がユニキャスト発見要求にのみ応答するようにします。

undo wlan capwap discovery-policy コマンドはデフォルトに戻します。

例

#ユニキャスト検出ポリシー機能を有効にします。

<AC> system-view

[AC] wlan capwap discovery-policy unicast

1.1.79 wlan global-configuration

Syntax

wlan global-configuration

View

System view

定義済みユーザロール

network-admin

説明

wlan global-configuration コマンドを使用して、Global configuration view に移行します。

AP の有効な設定は、AP、AP group、およびグローバル設定のうち、AP view 設定、AP group view 設定、Global configuration view の優先度が高い順に最も高い設定によって異なります。優先度の高い設定が存在しない場合、AP は優先度の低い設定を使用します。AP の構成が存在しない場合は、最も優先度の低い view のデフォルト値が使用されます。

例

#global configuration view に移動します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration]

1.1.80 wlan image-load filepath

Syntax

wlan image-load filepath { local | ram }

undo wlan image-load filepath

デフォルト

RAM

View

System view

定義済みユーザロール

network-admin

パラメータ

local:AP イメージファイルを優先して取得する場所としてローカルフォルダを指定します。ローカルフォルダに AP イメージファイルが含まれていない場合、AC は RAM から AP イメージファイルを取得します。RAM に AP イメージファイルが含まれていない場合、AC は AP イメージファイルを取得することはできません。

ram:AP イメージファイルを優先して取得する場所として RAM を指定します。RAM に AP イメージファイルが含まれていない場合、AC はローカルフォルダから AP イメージファイルを取得します。ローカルフォルダに AP イメージファイルが含まれていない場合、AC は AP イメージファイルを取得することはできません。

説明

AC のイメージファイルには AP イメージファイルが含まれています。AC は、起動時に AP イメージファイルを RAM に読み込みます。

local キーワードは、次の条件を満たす場合にだけ指定します。

- 必要な AP イメージファイルが AC のイメージファイルに含まれていない。
- AP がオンラインになるときに使用するソフトウェアバージョンが、**wlan apdb** コマンドを使用して指定されている。

local キーワードを指定する場合は、AC がデフォルトのファイルシステムとして AP イメージファイルが AC 上のファイルシステムのルートディレクトリに保存されていることを確認してください。

AC は、.ipe の AP イメージファイルのみを AP に割り当てることができます。

例

AP イメージファイルを優先して取得する場所として、AC のローカルフォルダを指定します。

<AC> system-view

[AC] wlan image-load filepath local

1.1.81 wlan re-group

Syntax

wlan re-group { **ap** *ap-name* | **ap-group** *source-group-name* |

mac-address *mac-address* | **serial-id** *serial-id* } *group-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*: AP 名で AP group ルールを指定します。

ap-group *old-group-name*: 送信元 AP group を指定します。送信元 AP group をデフォルト AP group にすることはできません。

mac-address *mac-address*: MAC アドレスで AP group ルールを指定します。

serial-id *serial-id*: シリアル ID で AP group ルールを指定します。

group-name: 宛先 AP group を指定します。宛先 AP group をデフォルト AP group にすることはできません。

説明

wlan re-group コマンドは AP group ルールまたは AP group ルールのリストを指定された AP group に移動します。

例

AP group group1 を作成し、ap1、ap2、ap3 という AP 名で AP group ルールを作成します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap ap1 ap2 ap3

[AC-wlan-ap-group-group1] quit

AP group group2 を作成し、AP 名で AP group ルールを group2 に移動します。

[AC] wlan ap-group group2

[AC-wlan-ap-group-group2] quit

[AC] wlan re-group ap ap1 group2

1.1.82 wlan rename-ap

Syntax

wlan rename-ap *ap-name new-ap-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

ap-name: 手動 AP を名前で指定します。大文字と小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を使用できます。

new-ap-name: 1～64 文字の大文字と小文字を区別しない新しい AP 名を指定します。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を使用できます。

説明

wlan rename-ap コマンドは手動 AP の名前を変更します。

例

AP ap1 の名前を ap1-office に変更します。

<AC> system-view

[AC] wlan rename-ap ap1 ap1-office

1.1.83 wlan tcp mss

Syntax

wlan tcp mss *value*

undo wlan tcp mss

デフォルト

1460 バイト

View

System view

定義済みユーザロール

network-admin

パラメータ

value: 128～2048 の範囲のバイト単位の TCP MSS を指定します。

説明

wlan tcp mss コマンドは CAPWAP トンネルの最大 TCP セグメントサイズ（MSS）を設定します。

undo wlan tcp mss コマンドはデフォルトに戻します。

このコマンドは、CAPWAP トンネルを介して送信される SYN パケットの MSS オプションの値を設定します。

MSS オプションは、送信者が受け入れることができる最大セグメントの受信者に通知します。各エンドは、TCP 接続の確立中に MSS をアナウンスします。TCP セグメントのサイズが受信側の MSS より小さいか等しい場合、TCP はフラグメンテーションなしで TCP セグメントを送信します。そうでない場合、TCP は受信者の MSS に基づいてセグメントを分割します。

例

#CAPWAP トンネルの TCP 最大セグメント長を 2000 バイトに設定します。

<AC> system-view

[AC] wlan tcp mss 2000

1.1.84 wlan timezone-sync enable

Syntax

wlan timezone-sync enable

undo wlan timezone-sync enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan timezone-sync enable コマンドは、タイムゾーンの同期を有効にします。

undo wlan timezone-sync enable コマンドは、デフォルトに戻します。

例

#タイムゾーンの同期を有効にします。

<Syname> system-view

[AC] wlan timezone-sync enable

目次

このセクションのページは **7-x-x** です。

2 章 コンフィグレーションプロファイルの設定 2-1
2.1 コンフィグレーションプロファイルの設定コマンド 2-1
2.1.1 acl 2-1
2.1.2 address range 2-3
2.1.3 authentication-mode 2-4
2.1.4 authorization-attribute 2-6
2.1.5 configuration profile 2-8
2.1.6 configuration-profile 2-9
2.1.7 dhcp enable 2-10
2.1.8 dhcp relay server-address 2-11
2.1.9 dhcp select 2-12
2.1.10 dhcp server ip-pool 2-13
2.1.11 dns-list 2-14
2.1.12 expired 2-15
2.1.13 forbidden-ip-range 2-16
2.1.14 gateway-list 2-17
2.1.15 interface 2-18
2.1.16 interface bridge-aggregation 2-18
2.1.17 interface vlan-interface 2-19
2.1.18 ip address 2-20
2.1.19 ip address dhcp-alloc 2-21
2.1.20 ip route-static 2-22
2.1.21 line 2-23
2.1.22 line class 2-24
2.1.23 local-user 2-25
2.1.24 network 2-27
2.1.25 packet-filter 2-28
2.1.26 password 2-29
2.1.27 port access vlan 2-30
2.1.28 port hybrid pvid 2-31
2.1.29 port hybrid vlan 2-32
2.1.30 port link-aggregation group 2-33
2.1.31 port link-type 2-34
2.1.32 port trunk permit vlan 2-35
2.1.33 port trunk pvid 2-36
2.1.34 port-isolate enable 2-38

2.1.35 qos priority 2-39
2.1.36 qos trust 2-39
2.1.37 rule (IPv4 advanced ACL view) 2-40
2.1.38 rule (IPv4 basic ACL view) 2-47
2.1.39 rule (Layer 2 ACL view) 2-48
2.1.40 rule comment 2-50
2.1.41 service-type 2-51
2.1.42 set authentication password 2-52
2.1.43 shutdown 2-54
2.1.44 step 2-55
2.1.45 telnet server enable 2-56
2.1.46 vlan 2-56

2章 コンフィグレーションプロファイルの設定

2.1 コンフィグレーションプロファイルの設定コマンド

🕮 **メモ**:

この章のコマンドは、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

2.1.1 acl

Syntax

acl number *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

acl { name *acl-name* | **number** *acl-number* [**name** *acl-name*] }

acl { **advanced** | **basic** } { *acl-number* | **name** *acl-name* }

acl mac { *acl-number* | **name** *acl-name* }

undo acl { all | **name** *acl-name* | **number** *acl-number* }

undo acl { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

basic: 標準 ACL を指定します。

advanced: 拡張 ACL を指定します。

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *acl-name*: ACL を識別しやすくするため、ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

all: すべての ACL を指定します。

説明

acl コマンドは ACL を作成し、ACL の view に移行します。すでに ACL が作成されている場合、その view に移行します。

undo acl コマンドは指定された、あるいはすべての ACL を削除します。

ACL のルールが一致順序を含む、あるいは以下の一致基準が有効である場合、一致するパケットはソフトウェアベースのパケット転送を行います。

- 送信元および宛先 IP アドレス
- 送信元ポート、宛先ポート
- トランスポートレイヤプロトコル
- ICMP メッセージタイプ、メッセージコード、およびメッセージ名
- VPN インスタンス
- ロギング
- タイムレンジ

ソフトウェアベースのパケット転送は、転送エントリのため、コントロールプレーンにパケットを送信します。これは装置のパケット転送に影響します。

例

コンフィグレーションプロファイル **ap1** に標準 IPv4 ACL 2000 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000]

コンフィグレーションプロファイル **ap1** に ACL 名が flow の標準 IPv4 ACL を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic name flow

[AC-config-profile-ap1-acl-ipv4-basic-flow]

コンフィグレーションプロファイル **ap1** に 拡張 IPv4 ACL 3000 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3000

[AC-config-profile-ap1-acl-ipv4-adv-3000]

コンフィグレーションプロファイル **ap1** に L2 ACL 4000 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl mac 4000

[AC-config-profile-ap1-acl-mac-4000]

コンフィグレーションプロファイル **ap1** に ACL 名が flow の L2 ACL を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl mac name flow

[AC-config-profile-ap1-acl-mac-flow]

2.1.2 address range

Syntax

address range *start-ip-address end-ip-address*

undo address range

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 開始 IP アドレスを指定します。

end-ip-address: 終了 IP アドレスを指定します。

説明

address range コマンドはダイナミックの割り当てを行うため DHCP アドレスプールの IP アドレス範囲を設定します。

undo address range コマンドは DHCP アドレスプールの IP アドレス範囲を削除します。

IP アドレス範囲が指定されていない場合、address pool view で **network** コマンドを使用してサブネットのすべての IP アドレスを割り当てることができます。IP アドレス範囲が指定されている場合、IP アドレス範囲の IP アドレスのみを割り当てることができます。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

address range で指定されたアドレス範囲は **network** コマンドで指定されたサブネット内にある必要があります。範囲外のアドレスを割り当てることはできません。

例

コンフィグレーションプロファイル **ap1** の DHCP アドレスプール 1 に 192.168.8.1～192.168.8.150 のアドレス範囲を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 1

[AC-config-profile-ap1-dhcp-pool-1] address range 192.168.8.1 192.168.8.150

関連コマンド

network

2.1.3 authentication-mode

Syntax

authentication-mode { **none** | **password** | **scheme** }

undo authentication-mode

デフォルト

VTY line の認証モードは password です。

コンソールユーザの認証モードは製品モデルにより異なります。

QX-W1000 シリーズは none です。

QX-W1100 シリーズは password です。

QX-W1200 シリーズは password です。

View

Configuration profile-user line view

Configuration profile-user line class view

定義済みユーザロール

network-admin

パラメータ

none: 認証を無効にします。

password: ローカルパスワード認証を行います。

scheme: AAA 認証を行います。AAA の詳細はオペレーションマニュアルのセクション 9 *セキュリティ　"AAA"* を参照してください。

説明

authentication-mode コマンドは user line の認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

network-admin またはレベル 15 ユーザの役割を割り当てられたユーザだけがこのコマンドを実行することができます。他のユーザがこのコマンドを実行する権利を与えられても、このコマンドを実行することができません。

認証モードが **none** である場合、すべてのユーザは認証なしでログインすることができます。装置のセキュリティを改善するため、認証モードを **password** あるいは **scheme** にしてください。

VTY line view で、**authentication-mode** コマンドは **protocol inbound** コマンドと関連します。VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

認証モードを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

コンフィグレーションプロファイル **ap1** の user line VTY 0 で認証モードを none にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line vty 0

[AC-config-profile-ap1-line-vty0] authentication-mode none

コンフィグレーションプロファイル **ap1** の user line VTY 0 で認証モードを password に設定し、パスワードを 321 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line vty 0

[AC-config-profile-ap1-line-vty0] authentication-mode password

[AC-config-profile-ap1-line-vty0] set authentication password simple 321

コンフィグレーションプロファイル **ap1** の user line VTY 0 で認証モードを scheme に設定します。ローカルユーザ 123 を設定し、パスワードを 321 に設定します。Telnet サービスを割り当て、ユーザのユーザロールを network-admin に割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line vty 0

[AC-config-profile-ap1-line-vty0] authentication-mode scheme

[AC-config-profile-ap1-line-vty0] quit

[AC-config-profile-ap1] local-user 123

[AC-config-profile-ap1-luser-manage-123] password simple 321

[AC-config-profile-ap1-luser-manage-123] service-type telnet

[AC-config-profile-ap1-luser-manage-123] authorization-attribute user-role network-admin

関連コマンド

set authentication password

2.1.4 authorization-attribute

Syntax

authorization-attribute { **idle-cut** *minutes* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **idle-cut** | **session-timeout** | **user-role** *role-name* | **vlan** | **work-directory** } *

デフォルト

FTP、SFTP ユーザは作業ディレクトリとして NAS のルートディレクトリを設定します。しかし、ユーザはルートディレクトリへのアクセス許可がありません。

network-admin あるいは level-15 のユーザによって作成されたローカルユーザは network-operator のユーザロールが割り当てられています。

View

Configuration profile-Local user view

定義済みユーザロール

network-admin

パラメータ

idle-cut *minute*: アイドルタイムアウト時間を設定します。設定範囲は 1～120 分です。指定されるアイドル時間を超過したアイドル中のオンラインユーザはログアウトされます。

user-role *role-name*: 許可されたユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザに 64 のユーザロールを指定することができます。このオプションは local user view でのみ有効で、user group view では無効です。

vlan *vlan-id*: 許可 VLAN を指定します。設定範囲は 1～4094 です。認証にパスし、VLAN が許可されたのち、ローカルユーザは VLAN のリソースのみアクセスすることができます。

work-directory *directory-name*: FTP、SFTP ユーザの作業ディレクトリを指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。このディレクトリは既に存在している必要があります。デフォルトで FTP、SFTP ユーザは装置のルートディレクトリにアクセスすることができます。

説明

authorization-attribute コマンドはローカルユーザまたはユーザグループの許可属性を設定します。ローカルユーザ、またはローカルユーザのユーザグループが認証を通過すると、装置はユーザにそれらの属性を割り当てます。

undo authorization-attribute コマンドはデフォルトに戻します。

アプリケーション環境と目的に従って許可属性を設定してください。ユーザのサービスタイプに依存して許可属性をサポートします。

SSH、Telnet、端末ユーザの場合、許可属性はアイドルカット、ユーザロール、作業ディレクトリが適用できます。

HTTP、HTTPS ユーザの場合、許可属性はユーザロールが適用できます。

FTP ユーザの場合、許可属性はアイドルカット、ユーザロール、作業ディレクトリが適用できます。

ローカルユーザのほかのタイプは適用されません。

ユーザが許可されたユーザロールのみ適用させるため、あらかじめ定義されたユーザロールを削除するために **undo authorization-attribute user-role** コマンドを使用してください。

例

コンフィグレーションプロファイル **ap1** に作成した装置管理ユーザ abc の許可される VLAN を VLAN 2 として設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user abc class network

[AC-config-profile-ap1-luser-network-abc] authorization-attribute vlan 2

2.1.5 configuration profile

Syntax

configuration profile *profile-name* **[model** *model-name* **]**

undo configuration profile *profile-name*

デフォルト

設定無し

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: コンフィグレーションプロファイルの名前を 1～64 文字の文字列で指定します。文字、数字、アンダースコア (_) 、ドット (。) 、左括弧 ([) 、右括弧 (]) 、スラッシュ (/) 、ハイフン (-) が使用可能です。大文字と小文字は区別されます。

model *model-name*: AP モデル名を指定します。このパラメータは、コンフィグレーションプロファイルを作成するときに必要です。

説明

configuration profile コマンドはコンフィグレーションプロファイルを作成し、その View に移行するか、既存のコンフィグレーションプロファイルの View に移行します。

undo configuration profile コマンドは、既存のコンフィグレーションプロファイルを削除します。

AC でコンフィグレーションプロファイルを作成し、プロファイルを 1 つまたは複数の AP に関連付けることができます。その後、AC はプロファイルで指定された設定を、関連付けられた AP がオンラインになったときに自動的に展開します。

コンフィグレーションプロファイルを作成するときは、AP モデル名を指定する必要があります。AC は、AP モデルに基づいてプロファイルにデフォルト設定を生成します。

AC には最大 2048 のコンフィグレーションプロファイルを作成することができます。

例

AP **ap1 model QX-W1130** のコンフィグレーションプロファイルを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1]

2.1.6 configuration-profile

メモ：

- **configuration-profile** と **remote-configuration** を同じ AP に対して設定しないでください。
- コンフィグレーションプロファイルで設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**configuration-profile** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

Syntax

configuration-profile *profile-name*

undo configuration-profile

デフォルト

設定無し

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

profile-name: コンフィグレーションプロファイルの名前を 1～64 文字の文字列で指定します。文字、数字、アンダースコア (_) 、ドット (。) 、左括弧 ([) 、右括弧 (]) 、スラッシュ (/) 、ハイフン (-) が使用可能です。大文字と小文字は区別されます。

説明

configuration-profile コマンドは、既存のコンフィグレーションプロファイルを AP または AP グループと関連付けます。

undo configuration-profile コマンドは、デフォルトに戻します。

既存のコンフィグレーションプロファイルを AP または AP グループに関連付けます。AP または AP グループ内の AP がオンラインになると、AC はプロファイル内の設定を AP に自動的に展開します。

コンフィグレーションプロファイルと AP または AP グループの関連付けを解除するには、undo configuration-profile コマンドを実行します。また、undo configuration-profile コ

マンドを実行すると、AP または AP グループ内の AP の設定が工場出荷時のデフォルトに復元されます。

例

AP **ap1 model QX-W1130** とコンフィグレーションプロファイル **profile1** を関連付けます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] configuration-profile profile1

AP グループ **apgroup1** の 型番 **QX-W1130** とコンフィグレーションプロファイル **profile1** を関連付けます。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] configuration-profile profile1

2.1.7 dhcp enable

Syntax

dhcp enable

undo dhcp enable

デフォルト

無効

View

Configuration profile view

定義済みユーザロール

network-admin

説明

dhcp enable コマンドは DHCP を有効にします。

undo dhcp enable コマンドは DHCP を無効にします。

DHCP に関する設定は DHCP を有効にしたのち適用されます。

DHCP サーバあるいは DHCP リレーエージェントの設定を実行する前に、DHCP を有効にしてください。

例

コンフィグレーションプロファイル **ap1** の DHCP を有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp enable

2.1.8 dhcp relay server-address

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: DHCP サーバの IP アドレスを指定します。DHCP リレーエージェントは DHCP クライアントから受信した DHCP パケットを DHCP サーバに転送します。

説明

dhcp relay server-address コマンドは DHCP リレーエージェントの DHCP サーバを指定します。

undo dhcp relay server-address コマンドは DHCP サーバを削除します。

DHCP サーバを指定する IP アドレスは、DHCP リレーエージェントインタフェースの IP アドレスと同一のサブネット上に置くことはできません。その場合、DHCP クライアントは IP アドレスの取得に失敗します。

インタフェースで最大 8 つの DHCP サーバを指定することができます。DHCP リレーエージェントはクライアントからのパケットをすべての指定された DHCP サーバに転送します。

IP アドレスを指定しない場合、**undo dhcp relay server-address** コマンドはインタフェースのすべての DHCP サーバを削除します。

例

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 10 で DHCP リレーエージェントの DHCP サーバアドレス 1.1.1.1 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] dhcp relay server-address 1.1.1.1

2.1.9 dhcp select

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

デフォルト

インタフェースは DHCP サーバモードで動作し、設定パラメータの DHCP 要求に応答します。

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

relay: インタフェースで DHCP リレーエージェントを有効にします。

server: インタフェースで DHCP サーバを有効にします。

説明

dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを有効にします。

undo dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを無効にします。無効にした場合、インタフェースは受信した DHCP パケットを廃棄します。

例

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 2 で DHCP リレーエージェントを有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 2

[AC-config-profile-ap1-Vlan-interface2] dhcp select relay

2.1.10 dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

pool-name: アドレスプールを固有に識別するため DHCP アドレスプールの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

dhcp server ip-pool コマンドは DHCP アドレスプールを作成し、その view に移行します。

undo dhcp server ip-pool コマンドは指定した DHCP アドレスプールを削除します。

またコマンドを使用して既存の DHCP アドレスプールに移行することができます。

DHCP アドレスプールは DHCP クライアントに割り当てられる設定パラメータを記録するために使用されます。

例

コンフィグレーションプロファイル **ap1** に DHCP アドレスプール pool1 を作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool pool1

[AC-config-profile-ap1-dhcp-pool-pool1]

関連コマンド

- **dhcp server apply ip-pool**
- **display dhcp server pool**

2.1.11 dns-list

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: DNS サーバを指定します。&<1-8>は DNS サーバのアドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを指定します。

undo dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

パラメータを指定しない場合、**undo dns-list** コマンドは DHCP アドレスプールのすべての DNS サーバのアドレスを削除します。

例

コンフィグレーションプロファイル **ap1** の DHCP アドレスプール 0 の DNS サーバアドレス 10.1.1.254 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] dns-list 10.1.1.254

関連コマンド

display dhcp server pool

2.1.12 expired

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

デフォルト

1 日

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

day *day*: 日数を指定します。設定範囲は 0～365 日です。

hour *hour*: 時間を指定します。設定範囲は 0～23 時間です。デフォルトは 0 時間です。

minute *minute*: 分を指定します。設定範囲は 0～59 分です。デフォルトは 0 分です。

second *second*: 秒を指定します。設定範囲は 0～59 秒です。デフォルトは 0 秒です。

unlimited: リース期間を指定しません。正確には 136 年のリース期間です。

説明

expired コマンドは DHCP アドレスプールのリース期間を指定します。

undo expired コマンドは DHCP アドレスプールのリース期間をデフォルトに戻します。

DHCP サーバは DHCP クライアントにリース期間とともに IP アドレスを割り当てます。リース期間が終了する前に、DHCP クライアントはリース期間を延長する必要があります。

- リース期間の延長が成功した場合、DHCP クライアントは IP アドレスを使用し続けることができます。
- リース期間の延長が失敗したとき、以下のイベントの両方が発生します。
  - □ リース期間が終了した後 DHCP クライアントは IP アドレスを使用することができません。
  - □ DHCP サーバは終了したアドレスとして IP アドレスにラベルをつけます。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のリース期間を 1 日、2 時間、3 分、4 秒に指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4

2.1.13 forbidden-ip-range

Syntax

forbidden-ip-range *start-ip-address* [*end-ip-address*]

undo forbidden-ip-range [*start-ip-address* [*end-ip-address*]]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 除外する IP アドレス範囲の開始アドレスを指定します

end-ip-address: 除外する IP アドレス範囲の終了アドレスを指定します

説明

forbidden-ip-range コマンドはアドレスプールのダイナミック割り当てから IP アドレス範囲を除外します。

undo forbidden-ip-range コマンドは設定を削除します。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のダイナミック割り当てから 192.168.10.1 から 192.168.10.10 のアドレス範囲を除外します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 1

[AC-config-profile-ap1-dhcp-pool-1] forbidden-ip-range 192.168.10.1 192.168.10.10

2.1.14 gateway-list

Syntax

gateway-list *ip-address*&<1-64>

undo gateway-list [*ip-address*&<1-64>]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-64>: ゲートウェイを指定します。&<1-64>はゲートウェイアドレスを半角スペースで区切り最大 64 つまで指定できることを示します。ゲートウェイアドレスは割り当て可能な IP アドレスと同一のサブネットに存在する必要があります。

説明

gateway-list コマンドは DHCP アドレスプールのゲートウェイアドレスを指定します。

undo gateway-list コマンドは DHCP アドレスプールからゲートウェイアドレスを削除します。

パラメータを指定しない場合、**undo gateway-list** コマンドはすべてのゲートウェイアドレスを削除します。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のゲートウェイアドレスに 10.1.1.1 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] gateway-list 10.1.1.1

2.1.15 interface

Syntax

interface *interface-type interface-number*

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

説明

interface コマンドは interface view に移行します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 の interface view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1]

2.1.16 interface bridge-aggregation

Syntax

interface bridge-aggregation *interface-number*

undo interface bridge-aggregation *interface-number*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

interface-number: アグリゲートインタフェースの番号を指定します。（1 で固定です。）

説明

interface bridge-aggregation コマンドはアグリゲートインタフェースを作成し、aggregate interface view に移行します。すでにアグリゲートインタフェースが存在する場合、aggregate interface view に移行します。

undo interface bridge-aggregation コマンドはアグリゲートインタフェースを削除します。

アグリゲートインタフェースを作成したとき、システムは自動的に同一番号のアグリゲーショングループを作成します。デフォルトのアグリゲーショングループはスタティックのアグリゲーションモードです。

アグリゲートインタフェースを削除するとアグリゲートグループも削除されます。同時にアグリゲーショングループのメンバポートがアグリゲーショングループから除外されます。

例

コンフィグレーションプロファイル **ap1** にアグリゲートインタフェース Bridge-Aggregation 1 を作成し、aggregate interface view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface bridge-aggregation 1

[AC-config-profile-ap1-Bridge-Aggregation1]

2.1.17 interface vlan-interface

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

interface-number: VLAN インタフェース番号を指定します。設定範囲は 1～4094 です。

説明

interface vlan-interface コマンドは VLAN インタフェースを作成し、作成された VLAN インタフェースの view に移行あるいは既存の VLAN インタフェースの view に移行します。

undo interface vlan-interface コマンドは VLAN インタフェースを削除します。

VLAN インタフェースを作成する前に、VLAN を作成してください。

例

コンフィグレーションプロファイル **ap1** に VLAN インタフェース 2 を作成し、作成された VLAN インタフェースの view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 2

[AC-config-profile-ap1-vlan2] quit

[AC-config-profile-ap1] interface vlan-interface 2

[AC-config-profile-ap1-Vlan-interface2]

2.1.18 ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* | *mask* } [**sub**]

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: インタフェースの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: サブネットマスクの長さを指定します。設定範囲は 1～31 です。

mask: サブネットマスクを指定します。ドットで区切り、10 進数で指定します。

sub: インタフェースにセカンダリ IP アドレスを割り当てます。

説明

ip address コマンドはインタフェースに IP アドレスを割り当てます。

undo ip address コマンドはインタフェースから IP アドレスを削除します。

インタフェースのプライマリ IP アドレスあるいはセカンダリ IP アドレスを設定するために、このコマンドを使用します。

インタフェースは 1 つのプライマリ IP アドレスのみ設定することができます。新しく設定されたプライマリ IP アドレスは、古いアドレスを上書きします。インタフェースが複数のサブネットに接続されている場合、サブネットがインタフェースを通して通信できるように、プライマリ IP アドレスとサブネットを設定します。

BOOTP、DHCP、PPP を通して IP アドレスを取得するインタフェースはセカンダリ IP アドレスを設定することができません。

undo ip address コマンドはインタフェースからすべての IP アドレスを削除します。

undo ip address *ip-address* { *mask* | *mask-length* }コマンドはプライマリ IP アドレスを削除します。**undo ip address** *ip-address* { *mask* | *mask-length* } **sub** コマンドはセカンダリ IP アドレスを削除します。

インタフェースに割り当てたプライマリ IP アドレスとセカンダリ IP アドレスは同一ネットワークセグメント上に設定することができますが、装置の異なるインタフェースは異なるネットワークセグメント上に存在する必要があります。

例

コンフィグレーションプロファイル **ap1** に 作成した VLAN インタフェース 10 にプライマリ IP アドレスを 129.12.0.1、セカンダリ IP アドレスを 202.38.160.1、サブネットマスクを 255.255.255.0 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] ip address 129.12.0.1 255.255.255.0

[AC-config-profile-ap1-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub

2.1.19 ip address dhcp-alloc

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

デフォルト

設定なし

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

説明

ip address dhcp-alloc コマンドは DHCP を使用して IP アドレスを取得するインタフェースを設定します。

undo ip address dhcp-alloc コマンドはインタフェースで DHCP の使用を停止します。

undo ip address dhcp-alloc コマンドを実行すると、インタフェースは DHCP を通して取得した IP アドレスをリリースするため、DHCP-RELEASE メッセージを送信します。インタフェースがダウンしている場合、メッセージを送信することができません。

例

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 10 に、 DHCP を使用して IP アドレスを取得する設定をします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 10

[AC-config-profile-ap1-Vlan-interface10] ip address dhcp-alloc

2.1.20 ip route-static

Syntax

ip route-static *dest-address* { *mask-length* | *mask* } *next-hop-address*

undo ip route-static *dest-address* { *mask-length* | *mask* } [*next-hop-address*]

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

dest-address: スタティックルートの宛先アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: IP アドレスのマスク長を指定します。設定範囲は 0～32 です。

mask: IP アドレスのマスクを指定します。ドットで区切り、10 進数で指定します。

next-hop-address: ネクストホップの IP アドレスを指定します。ドットで区切り、10 進数で指定します。詳細はオペレーションマニュアルのセクション 6 *ルーティングプロトコル “スタティックルーティング”* を参照してください。

説明

ip route-static コマンドはスタティックルートを設定します。

undo ip route-static コマンドはスタティックルートを削除します。

宛先アドレスとマスクの両方が 0.0.0.0（あるいは 0）である場合、設定されたルートはデフォルトルートです。デフォルトルートはルーティングテーブルに一致するエントリがないパケットを転送するのに使用されます。

例

コンフィグレーションプロファイル **ap1** に宛先アドレスが 1.1.1.1/24、ネクストホップが 2.2.2.2、のスタティックルートを設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] ip route-static 1.1.1.1 24 2.2.2.2

2.1.21 line

Syntax

line { **console** | **vty** } *first-number* [*last-number*] }

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

console *first-number*: first console line の相対番号を指定します。

vty *first-number*: first VTY line の相対番号を指定します（0～63）。

vty *last-number*: last VTY user line の相対番号を指定します（1～63）。*first-number* よりも小さくすることはできません。

説明

line コマンドは 1 つ以上の user line view に移行します。

シングル user line に設定を行うために、このコマンドを使用して user line view に移行します。

同じ設定を複数の user line に行うために、このコマンドを使用して複数の user line view に移行します。

例

コンフィグレーションプロファイル **ap1** の user line Console 0 の view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1] line console 0

[AC-config-profile-ap1-line-console0]

コンフィグレーションプロファイル **ap1** の user lines VTY 0～VTY 4 の view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1130

[AC-config-profile-ap1] line vty 0 4

[AC-config-profile-ap1-line-vty0-4]

関連コマンド

line class

2.1.22 line class

Syntax

line class { **console** | **vty** }

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

console: console line class view を指定します。

vty: VTY line class view を指定します。

説明

line class コマンドは user line class view に移行します。

line class のすべての user line で設定を同一にするために、user line class view に移行します。

user line class view では以下のコマンドを実行することができます。

- **authentication-mode**
- **set authentication password**

いくつかのログインコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定は user line で適用されます。user line class view の設定は class のすべての user line で適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。
- user line view の設定はすぐに適用され、オンラインユーザに影響します。user line class view の設定は設定が完了したのちにログインしたユーザのみ適用されます。user line class view の設定はオンラインユーザに影響しません。

例

コンフィグレーションプロファイル **ap1** の VTY line class view で認証モードを none にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line class vty

[AC-config-profile-ap1-line-class-vty] authentication-mode none

関連コマンド

line

2.1.23 local-user

Syntax

local-user *user-name* [**class manage**]

undo local-user { *user-name* **class manage** | **all** [**service-type** { **ftp** | **http** | **https | ssh** | **telnet** | **terminal** } | **class manage**] }

デフォルト

設定なし

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*: ローカルユーザ名を指定します。設定範囲は 1～55 です。大文字、小文字を区別します。

- ドメイン名を含めることはできません。
- スラッシュ（/），バックスラッシュ、垂直バー（|）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）
- （a）、（al）、（all）は使用できません。

class: ローカルユーザタイプを指定します。指定しない場合、装置管理ユーザを指定します。

- **manage**: 装置管理ユーザを指定します。装置管理ユーザは FTP、HTTP、HTTPS、SSH、Telnet、端末サービスを使用することができます。

all: すべてのユーザを指定します。

service-type: ローカルユーザの使用するサービスタイプを指定します。

- **ftp**: FTP ユーザを指定します。
- **http**: HTTP ユーザを指定します。
- **https**: HTTPS ユーザを指定します。
- **ssh**: SSH ユーザを指定します。
- **telnet**: Telnet ユーザを指定します。
- **terminal**: コンソールポートを使用してログインする端末ユーザを指定します。

説明

local-user コマンドはローカルユーザを追加し、local user view に移行します。

undo local-user コマンドはローカルユーザを削除します。

Configuration profile view では装置管理ユーザのみ作成することができ、最大 16 の装置管理ユーザが作成することができます。

例

コンフィグレーションプロファイル **ap1** に装置管理ユーザ user1 を追加し、local user view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user user1 class manage

[AC-config-profile-ap1-luser-manage-user1]

関連コマンド

service-type

2.1.24 network

Syntax

network *network-address* [*mask-length* | **mask** *mask*]

undo network *network-address* [*mask-length* | **mask** *mask*]

デフォルト

設定なし

View

Configuration profile-DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

network-address: ダイナミック割り当てのサブネットを指定します。マスク長やマスクが指定されない場合、ナチュラルマスクが使用されます。

mask-length: マスク長を指定します。設定範囲は 1～30 です。

mask *mask*: ドットで区切られた形式でマスクを指定します。

説明

network コマンドは DHCP アドレスプールのダイナミック割り当てのサブネットを指定します。

undo network コマンドは指定されたサブネットを削除します。

DHCP アドレスプールで 1 つのプライマリサブネットのみを指定することができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

ネットワークの設定の変更あるいは削除を行うと現在のアドレスプールから割り当てられたアドレスを削除します。

例

コンフィグレーションプロファイル **ap1** に作成した DHCP アドレスプール 0 のサブネットとして 192.168.8.0/24 を指定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] dhcp server ip-pool 0

[AC-config-profile-ap1-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0

関連コマンド

gateway-list

2.1.25 packet-filter

Syntax

packet-filter [mac] { *acl-number* **| name** *acl-name* **} { inbound | outbound }**

undo packet-filter [mac] { *acl-number* **| name** *acl-name* **} { inbound | outbound }**

デフォルト

設定なし

View

Configuration profile- interface view

定義済みユーザロール

network-admin

パラメータ

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *acl-name*: ACL を識別しやすくするため、ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

inbound: インタフェースで受信されるパケットをフィルタリングします。

outbound: インタフェースで送信されるパケットをフィルタリングします。

説明

packet-filter コマンドはパケットをフィルタするため、インタフェースに ACL を適用します。

undo packet-filter コマンドはインタフェースから ACL を削除します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 に受信トラフィックをフィルタするため、標準 IPv4 ACL 2001 を適用します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] packet-filter 2001 inbound

2.1.26 password

Syntax

password [{ **hash** | **simple** } *string*]

undo password

デフォルト

ローカルユーザのパスワードは設定されていません。正しいユーザ名を入力し、属性の確認を行った後、認証にパスできます。

View

Configuration profile-Local user view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号テキストのパスワードを設定します。

hash: ハッシュパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

string: パスワードを指定します。大文字、小文字を区別します。

- ハッシュテキストのパスワードは 1～110 文字です。
- プレーンテキストのパスワードは 1～63 文字です。

🕮 **メモ：**

string は以下の要件を満たす文字列にしてください。

- 10 文字以上。
- アルファベット、数字、記号のうち 2 種類以上を含む。
- ユーザ名またはユーザ名の逆の文字を含まない。

説明

password コマンドはローカルユーザのパスワードを設定します。

undo password コマンドはローカルユーザのパスワードを削除します。

プレーンテキストパスワードとハッシュパスワードをサポートします。

例

コンフィグレーションプロファイル **ap1** に 装置管理ユーザ user1 のパスワード 123456TESTplat&!をプレーンテキストで設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user user1 class manage

[AC-config-profile-ap1-luser-manage-user1] password simple 123456TESTplat&!

2.1.27 port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

すべてのアクセスポートは VLAN1 に所属しています。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port access vlan コマンドはアクセスポートを指定した VLAN に割り当てます。

undo port access vlan コマンドはデフォルトに戻します。

アクセスポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 に VLAN 3 を割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 3

[AC-config-profile-ap1-vlan3] quit

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port access vlan 3

2.1.28 port hybrid pvid

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートの PVID はポートが所属している VLAN の ID です。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port hybrid pvid コマンドはハイブリッドポートの PVID を設定します。

undo port hybrid pvid コマンドはハイブリッドポートの PVID を 1 に設定します。

ハイブリッドポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドでハイブリッドポートの PVID を削除する場合、ポートの PVID の設定は適用されません。

ローカルとリモートのハイブリッドポートに同じ PVID を設定することを推奨します。

PVID からのパケットの転送を許可するためにハイブリッドポートの設定に **port hybrid pvid** コマンドを使用してください。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をハイブリッドポートに設定します。PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 をタグ無しメンバとして割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 100

[AC-config-profile-ap1-vlan100] quit

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type hybrid

[AC-config-profile-ap1-GigabitEthernet1/0/1] port hybrid pvid vlan 100

[AC-config-profile-ap1-GigabitEthernet1/0/1] port hybrid vlan 100 untagged

関連コマンド

- **port hybrid vlan**
- **port link-type**

2.1.29 port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートはポートが所属している VLAN のタグなしメンバです。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

tagged: ポートは VLAN タグを削除しないで指定した VLAN のパケットを送信するように設定します。

untagged: ポートは VLAN タグを削除したのち、指定した VLAN のパケットを送信するように設定します。

説明

port hybrid vlan コマンドは指定した VLAN にハイブリッドポートを割り当てます。

undo port hybrid vlan コマンドは指定した VLAN からハイブリッドポートを削除します。

ハイブリッドポートは、複数の VLAN が通過できます。**port hybrid vlan** コマンドを繰り返し実行すると、ハイブリッドポートを通過する VLAN は、各実行の *vlan-id-list* により指定された VLAN に設定されます。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をハイブリッドポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当て、これらの VLAN のパケットにタグを付けて送信するよう GigabitEthernet 1/0/1 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type hybrid

[AC-config-profile-ap1-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

port link-type

2.1.30 port link-aggregation group

Syntax

port link-aggregation group *number*

undo port link-aggregation group

デフォルト

設定なし

View

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

number: アグリゲーショングループに対応するアグリゲートインタフェースの数を指定します。（1 で固定です。）

説明

port link-aggregation group コマンドは指定したアグリゲーショングループにインタフェースを割り当てます。

undo port link-aggregation group コマンドは所属しているアグリゲーショングループからインタフェースを削除します。

インタフェースは 1 つのアグリゲーショングループのみ所属することができます。

例

コンフィグレーションプロファイル **ap1** の アグリゲーショングループ 1 に GigabitEthernet 1/0/1 を割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-aggregation group 1

2.1.31 port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

access

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートのリンクタイプをアクセスとして指定します。

hybrid: ポートのリンクタイプをハイブリッドとして指定します。

trunk: ポートのリンクタイプをトランクとして指定します。

説明

port link-type コマンドはポートのリンクタイプを設定します。

undo port link-type コマンドはデフォルトに戻します。

トランクポートからハイブリッドポート（またはその逆）のリンクタイプを変更するには、まずリンクタイプをアクセスに設定する必要があります。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 のリンクタイプをトランクポートに設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type trunk

2.1.32 port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

トランクポートは VLAN 1 からのパケットのみ通過できるように許可します。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべての VLAN を通過できるように許可します。許可されていない VLAN ユーザがポートを通して制限されたリソースにアクセスすることを防ぐため､注意して **port trunk permit vlan all** コマンドを使用してください。

説明

port trunk permit vlan コマンドはトランクポートを指定した VLAN に割り当てます。

undo port trunk permit vlan コマンドはトランクポートを指定した VLAN から削除します。

トランクポートは複数の VLAN を通過できます。**port trunk permit vlan** コマンドを繰り返し実行すると、トランクポートを通過する VLAN は、各 *vlan-id-list* により指定された VLAN に設定されます。

トランクポート上では、PVID のトラフィックのみタグなしで通過することができます。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をトランクポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当てます。

```
<AC> system-view
[AC] configuration profile ap1 model QX-W1030
[AC-config-profile-ap1] interface GigabitEthernet 1/0/1
[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type trunk
[AC-config-profile-ap1-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100
```

関連コマンド

port link-type

2.1.33 port trunk pvid

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

VLAN 1

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port trunk pvid コマンドはトランクポートの PVID を設定します。

undo port trunk pvid コマンドはデフォルトに戻します。

トランクポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドを使用してトランクポートの PVID を削除しても、ポートの PVID の設定には影響しません。

ローカルおよびリモートのトランクポートは、PVID のトラフィックが正常に送信されるために同じ PVID を使用する必要があります。

PVID からのパケットの転送を許可するためにトランクポートの設定に **port trunk permit vlan** コマンドを使用してください。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をトランクポートに設定します。PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 を割り当てます。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port link-type trunk

[AC-config-profile-ap1-GigabitEthernet1/0/1] port trunk pvid vlan 100

[AC-config-profile-ap1-GigabitEthernet1/0/1] port trunk permit vlan 100

関連コマンド

- **port link-type**
- **port trunk permit vlan**

2.1.34 port-isolate enable

Syntax

port-isolate enable

undo port-isolate enable

デフォルト

Layer2 Ethernet interface view では、ポートアイソレーションは有効です。

Layer2 Aggregate interface view では、ポートアイソレーションは無効です。

View

Configuration profile-Layer 2 aggregate interface view

Configuration profile-Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

port-isolate enable コマンドはポートアイソレーションを有効にします。

undo port-isolate コマンドはポートアイソレーションを無効にします。

Ethernet interface view での設定は、そのインタフェースにのみ適用されます。

aggregate interface view での設定は、アグリゲートインタフェースとアグリゲーションメンバポートに適用されます。装置がアグリゲートインタフェースへの設定の適用に失敗した場合、装置はどのアグリゲーションメンバポートもアイソレーショングループに割り当てません。設定の適用失敗がアグリゲーションメンバポートで起きた場合、装置は失敗が起きたポートをスキップし、別のアグリゲーションメンバポートをアイソレーショングループに割り当てます。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] port-isolation enable

コンフィグレーションプロファイル **ap1** のアグリゲートインタフェース Bridge-Aggregation 1 でポートアイソレーションを有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface Bridge-Aggregation 1

[AC-config-profile-ap1-Bridge-Aggregation-1] port-isolate enable

2.1.35 qos priority

Syntax

qos priority *priority-value*

undo qos priority

デフォルト

0

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティの値を指定します。設定範囲は 0～7 です。

説明

qos priority コマンドはインタフェースのポートプライオリティを変更します。

undo qos priority コマンドはデフォルトに戻します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 のポートプライオリティを 2 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface gigabitethernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] qos priority 2

2.1.36 qos trust

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

デフォルト

インタフェースはパケットのプライオリティを信用しません。802.1p プライオリティとしてポートプライオリティを使用します。

View

Configuration profile-Interface view

定義済みユーザロール

network-admin

パラメータ

dot1p: プライオリティマッピングの受信パケットの 802.1p プライオリティを使用します。

dscp: プライオリティマッピングの受信パケットの DSCP を使用します。

説明

qos trust コマンドはインタフェースのプライオリティトラステッドモードを設定します。

undo qos trust コマンドはデフォルトのプライオリティのトラステッドモードに戻します。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 のプライオリティトラステッドモードを 802.1p プライオリティに設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface gigabitethernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] qos trust dot1p

2.1.37 rule (IPv4 advanced ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * } | **fragment** | **icmp-type** | **source** | **source-port** | **time-range**] *

undo rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** | **time-range** *time-range-name*] *

デフォルト

設定なし

View

Configuration profile-IPv4 advanced ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

protocol: プロトコル番号あるいはプロトコル名を指定します。

- プロトコル番号の設定範囲は 0～255 です。
- プロトコル名は **gre** (47)、**icmp** (1)、**igmp** (2)、**ip**、**ipinip** (4)、**ospf** (89)、**tcp** (6)、**udp** (17)を指定できます。**ip** はすべてのプロトコルを指定します。表 2-1 にプロトコルの値に関わらず指定できるパラメータを示します。

表 2-1 拡張 IPv4 ACL ルールの一致基準と他のルールの情報

パラメータ	機能	説明
source { *source-address source-wildcard* | **any** }	送信元アドレスを定義します。	*source-address*と*source-wildcard*はドットで区切られた10進数表記の送信元IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。 **any**は、任意の送信元IPアドレスを示します。
destination { *dest-address dest-wildcard* | **any** }	宛先アドレスを定義します。	*dest-address*と*dest-wildcard*はドットで区切られた10進数表記の宛先IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。 **any**は、任意の宛先IPアドレスを示します。
precedence *precedence*	IPプレシーデンスの値を指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～7です。名前は**routine** (0)、**priority** (1)、**immediate** (2)、**flash** (3)、**flash-override** (4)、**critical** (5)、**internet** (6)、**network** (7)が指定できます。
tos *tos*	ToSプレシーデンスを指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～15です。名前は**max-reliability** (2)、**max-throughput** (4)、**min-delay** (8)、**min-monetary-cost** (1)、**normal** (0)が指定できます。
dscp *dscp*	DSCPプライオリティを指定します。	*dscp*プライオリティの値あるいはプライオリティの名前を指定します。番号の設定範囲は0～63です。名前は**af11** (10)、**af12** (12)、**af13** (14)、**af21** (18)、**af22** (20)、**af23** (22)、**af31** (26)、**af32** (28)、**af33** (30)、**af41** (34)、**af42** (36)、**af43** (38)、**cs1** (8)、**cs2** (16)、**cs3** (24)、**cs4** (32)、**cs5** (40)、**cs6** (48)、**cs7** (56)、**default** (0)、**ef** (46)が指定できます。
fragment	最初のフラグメントではないフラグメントを指定します。	指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。

パラメータ	機能	説明
time-range *time-range-name*	ルールのタイムレンジを指定します。	*time-range-name*の設定範囲は1～32文字です。大文字、小文字を区別しません。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション8 *ACL and QoS* *“タイムレンジ”*を参照してください。

protocol が **tcp** (6)あるいは **udp** (17)である場合、設定するパラメータを表 2-2 に示します。

表 2-2 拡張 IPv4 ACL ルールの TCP/UDP 指定パラメータ

パラメータ	機能	説明
source-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの送信元ポート番号を指定します。	*operator*は**lt** (lower than)、**gt** (greater than)、**eq** (equal to)、**neq** (not equal to)、**range** (inclusive range)が指定できます。*port1*、*port2*はTCPあるいはUDPポート番号です。設定範囲は0～65535です。*port2*は*operator*が範囲であるときのみ必要です。 TCPポート番号は以下の名前で指定できます。**chargen** (19)、**bgp** (179)、**cmd** (514)、**daytime** (13)、**discard** (9)、**domain** (53)、**echo** (7)、**exec** (512)、**finger** (79)、**ftp** (21)、**ftp-data** (20)、**gopher** (70)、**hostname** (101)、**irc** (194)、**klogin** (543)、**kshell** (544)、**login** (513)、**lpd** (515)、**nntp** (119)、**pop2** (109)、**pop3** (110)、**smtp** (25)、**sunrpc** (111)、**tacacs** (49)、**talk** (517)、**telnet** (23)、**time** (37)、**uucp** (540)、**whois** (43)、**www** (80) UDPポート番号は以下の名前で指定できます **biff** (512)、**bootpc** (68)、**bootps** (67)、**discard** (9)、**dns** (53)、**dnsix** (90)、**echo** (7)、**mobilip-ag** (434)、**mobilip-mn** (435)、**nameserver** (42)、**netbios-dgm** (138)、**netbios-ns** (137)、**netbios-ssn** (139)、**ntp** (123)、**rip** (520)、**snmp** (161)、**snmptrap** (162)、**sunrpc** (111)、**syslog** (514)、**tacacs-ds** (65)、**talk** (517)、**tftp** (69)、**time** (37)、**who** (513)、**xdmcp** (177)
destination-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの宛先ポート番号を指定します。	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* |	ACK、FIN、PSH、RST、SYN、URGを	TCP用のパラメータです。各値は0(フラグビットがセットされていません)または1(フラグ

パラメータ	機能	説明
rst *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	含む1つまたは複数のTCPフラグを指定します。	ビットがセットされています)が指定できます。ルールのTCPフラグはANDの関係です。たとえば、ack 0 psh 1が設定されたルールは、ACKフラグが設定されていないパケット、およびPSHフラグが設定されているパケットに一致します。
established	TCP接続の確立状態を示すフラグを指定します。	TCP用のパラメータです。ルールはACKあるいはRSTフラグがセットされているTCP接続パケットに一致します。

protocol が **icmp** (1)である場合、設定するパラメータを表 2-3 に示します。

表 2-3 拡張 IPv4 ACL ルールの ICMP 指定パラメータ

パラメータ	機能	説明
icmp-type { **icmp-type** *icmp-code* | *icmp-message* }	ICMPメッセージタイプとコードを指定します。	*icmp-type*の設定範囲は0～255です。*icmp-code*の設定範囲は0～255です。*icmp-message*はメッセージの名前を指定します。サポートされるICMPメッセージ名と対応するタイプとコードの値を表 2-4に示します。

表 2-4 拡張 IPv4 ACL ルールでサポートされる ICMP メッセージ名

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

説明

rule コマンドは拡張 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは拡張 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

例

コンフィグレーションプロファイル **ap1** にアドレス 129.9.0.0/16 から 202.38.160.0/24 の宛先ポート 80 の TCP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3000

[AC-config-profile-ap1-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80

コンフィグレーションプロファイル **ap1** に 192.168.1.0/24 宛の ICMP パケットを除くすべての IP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3001

[AC-config-profile-ap1-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-adv-3001] rule permit ip

コンフィグレーションプロファイル **ap1** に FTP の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3002

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp

[AC-config-profile-ap1-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data

コンフィグレーションプロファイル **ap1** に SNMP と SNMP trap の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl advanced 3003

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp source-port eq snmp

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp

[AC-config-profile-ap1-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap

関連コマンド

- **acl**
- **step**
- **time-range**

2.1.38 rule (IPv4 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**fragment** | **source** | **time-range**] *

undo rule [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

デフォルト

設定なし

View

Configuration profile-IPv4 basic ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

fragment: 最初のフラグメントではないフラグメントを指定します。指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。

source { *source-address source-wildcard* | **any** }: 送信元アドレスを定義します。*source-address* と *source-wildcard* はドットで区切られた 10 進数表記の送信元 IP アドレスとワイルドカードマスクを示します。すべてが 0 のワイルドカードはホストアドレスを示します。**any** は、任意の送信元 IP アドレスを示します。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* *“タイムレンジ”* を参照してください。

説明

rule コマンドは標準 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは標準 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

例

コンフィグレーションプロファイル **ap1** に　アドレス 10.0.0.0/8、172.17.0.0/16、192.168.1.0/24 を除く送信元 IP セグメントからのパケットを拒否する標準 IPv4 ACL ルールを作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule deny source any

関連コマンド

- **acl**
- **step**
- **time-range**

2.1.39 rule (Layer 2 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**time-range**]

undo rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

デフォルト

設定なし

View

Configuration profile-Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

cos *vlan-pri*: 802.1p プライオリティを定義します。

- プライオリティの設定範囲は 0～7 です。
- **best-effort** (0)、**background** (1)、**spare** (2)、**excellent-effort** (3)、**controlled-load** (4)、**video** (5)、**voice** (6)、**network-management** (7)の用語で定義することができます。

dest-mac *dest-address dest-mask*: 宛先 MAC アドレス範囲を定義します。*dest-address* と *dest-mask* は宛先 MAC アドレスとマスクを示します。マスクの形式は H-H-H です。

lsap *lsap-type lsap-type-mask*: LLC カプセル化の DSAP と SSAP フィールドを定義します。*lsap-type* は 16 進数表記でカプセル化フォーマットを示します。*lsap-type-mask* は 16 進数表記で LSAP マスクを示します。

type *protocol-type protocol-type-mask*: L2 の 1 つ以上のプロトコルを定義します。*protocol-type* は 16 進数表記で Ethernet_II と Ethernet_SNAP のプロトコルタイプを示します。*protocol-type-mask* は 16 進数表記でプロトコルタイプのマスクを示します。

source-mac *source-address source-mask*: 送信元 MAC アドレス範囲を定義します。*source-address* は送信元 MAC アドレスを示します。*sour-mask* はマスクを示します。マスクの形式は H-H-H です。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 8 *ACL and QoS* *“タイムレンジ”* を参照してください。

説明

rule コマンドは L2 ACL のルールを作成あるいは修正します。

undo rule コマンドは L2 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

- すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。
- パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

L2 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

例

L2 ACL 4000 のルールを作成します。ARP パケットを許可し、RARP パケットを拒否します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] rule permit type 0806 ffff

[AC-config-profile-ap1-acl-mac-4000] rule deny type 8035 ffff

関連コマンド

- **acl**
- **step**

2.1.40 rule comment

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

デフォルト

設定なし

View

Configuration profile-IPv4 basic/advanced ACL view

Configuration profile-Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ACL のルール ID を指定します。設定範囲は 0～65534 です。ACL のルールはすでに作成されている必要があります。

text: ACL のルールの説明を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rule comment コマンドは ACL のルールの説明を設定します。

undo rule comment コマンドは ACL のルールの説明を削除します。

例

標準 IPv4 ACL 2000 を作成し、ルールの説明を追加します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0

[AC-config-profile-ap1-acl-ipv4-basic-2000] rule 0 comment This rule is used on Gigabitethernet 1/0/1.

2.1.41 service-type

Syntax

service-type { **ftp** | { **telnet** | **terminal** } * }

undo service-type { **ftp** | { **telnet** | **terminal** } * }

デフォルト

ローカルユーザは許可されておらず、サービスを使用することができません。

View

Configuration profile-Local user view

定義済みユーザロール

network-admin

パラメータ

ftp: ユーザが FTP サービスを使用することを許可します。許可されたディレクトリは **authorization-attribute work-directory** コマンドで変更することができます。

telnet: ユーザが Telnet サービスを使用することを許可します。

terminal: ユーザが端末サービスを使用し、コンソールポートからログインすることを許可します。

説明

service-type コマンドはローカルユーザが使用するサービスタイプを指定します。

undo service-type コマンドはローカルユーザが使用するサービスタイプを削除します。

複数のサービスタイプをユーザに割り当てることができます。

例

コンフィグレーションプロファイル **ap1** に作成した 装置管理ユーザ user1 が Telnet、FTP サービスを使用することを許可します。

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] local-user user1 class manage

[AC-config-profile-ap1-luser-manage-user1] service-type telnet

[AC-config-profile-ap1-luser-manage-user1] service-type ftp

2.1.42 set authentication password

Syntax

set authentication password { **hash** | **simple** } *password*

undo set authentication password

デフォルト

コンソールユーザのパスワード設定は AP モデルにより異なります。

QX-W1000 シリーズは設定なしです。

QX-W1100 シリーズは qx_admin です。

QX-W1200 シリーズは qx_admin です。

line class vty のパスワード設定は AP モデルにより異なります。

QX-W1000 シリーズは設定なしです。

QX-W1100 シリーズは qx_admin です。

QX-W1200 シリーズは qx_admin です。

View

Configuration profile-user line view

Configuration profile-user line class view

定義済みユーザロール

network-admin

パラメータ

hash: 暗号テキストのパスワードを設定します。

Simple: プレーンテキストのパスワードを設定します。

Password: 大文字、小文字が区別されたパスワードを指定します。**Simple** が指定された場合、設定範囲は 1～16 文字です。**Hash** が指定された場合、設定範囲は 1～110 文字です。

説明

set authentication password コマンドはパスワード認証のパスワードを設定します。

Undo set authentication password コマンドはパスワードを削除します。

セキュリティのため、保存されたパスワードは設定に関わらず常に暗号テキストで表示されます。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

例

コンフィグレーションプロファイル **ap1** の user line Console 0 でパスワード認証のパスワード hello を設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] line console 0

[AC-line-console0] authentication-mode password

[AC-line-console0] set authentication password simple hello

関連コマンド

authentication-mode

2.1.43 shutdown

Syntax

shutdown

undo shutdown

デフォルト

インタフェースはアップ状態です。

View

Configuration profile-interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはインタフェースをシャットダウンします。

Undo shutdown コマンドはインタフェースをアップします。

例

コンフィグレーションプロファイル **ap1** の GigabitEthernet 1/0/1 をシャットダウンし、それからアップします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface GigabitEthernet 1/0/1

[AC-config-profile-ap1-GigabitEthernet1/0/1] shutdown

[AC-config-profile-ap1-GigabitEthernet1/0/1] undo shutdown

コンフィグレーションプロファイル **ap1** の アグリゲートインタフェース Bridge-Aggregation 1 を up にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface bridge-aggregation 1

[AC-config-profile-ap1-Bridge-Aggregation1] undo shutdown

コンフィグレーションプロファイル **ap1** の VLAN インタフェース 2 をシャットダウンし、up にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] interface vlan-interface 2

[AC-config-profile-ap1-Vlan-interface2] shutdown

[AC-config-profile-ap1-Vlan-interface2] undo shutdown

2.1.44 step

Syntax

step *step-value*

undo step

デフォルト

ACL のルール番号付けステップは 5 で、開始ルール ID は 0 です。

View

Configuration profile-Ipv4 basic/advanced ACL view

Configuration profile-Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

step-value: ACL ルールのステップ数を指定します。設定範囲は 1～20 です。

説明

step コマンドは ACL ルールに自動的に番号を割り振るためのステップ数を設定します。

Undo step コマンドはデフォルトに戻します。

ルールの番号づけステップはシステムが自動的にルール番号の増分を設定します。たとえば、デフォルトの ACL の番号づけステップは 5 です。ルールを作成するとき、ID を割り当てない場合、ルールの番号は 0、5、10、15、…と番号づけられます。番号づけのステップを広くする場合、2 つのルールの間に多くのルールを挿入することができます。ステップを変更したときはいつでも、ルールは 0 から再ナンバリングが行われます。たとえば、5 つのルールの番号 5、10、13、15、20 がつけられている場合、ステップを 5 から 2 に変更すると、ルールの番号は 0、2、4、6、8 に再ナンバリングされます。

例

コンフィグレーションプロファイル **ap1** に作成した 標準 IPv4 ACL 2000 のステップ数を 2 に設定します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] acl basic 2000

[AC-config-profile-ap1-acl-ipv4-basic-2000] step 2

2.1.45 telnet server enable

Syntax

telnet server enable

undo telnet server enable

デフォルト

デフォルトは AP モデルにより異なります。

QX-W1000 シリーズでは無効です。

QX-W1100 シリーズでは有効です。

QX-W1200 シリーズでは有効です。

View

Configuration profile view

定義済みユーザロール

network-admin

説明

telnet server enable コマンドは Telnet サーバ機能を有効にします。

undo telnet server enable コマンドは Telnet サーバ機能を無効にします。

管理者は Telnet サーバ機能が有効であるときのみ装置に Telnet を行うことができます。

例

Telnet サーバ機能を有効にします。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] telnet server enable

2.1.46 vlan

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

デフォルト

VLAN 1（システムデフォルト VLAN）

View

Configuration profile view

定義済みユーザロール

network-admin

パラメータ

vlan-id1, vlan-id2: VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN の範囲を指定します。*vlan-id1* と *vlan-id2* は VLAN ID を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: VLAN 1～4094 を指定します。

説明

vlan *vlan-id* コマンドは VLAN を作成し、その view あるいは既存の VLAN の view に移行します。

vlan *vlan-id1* **to** *vlan-id2* コマンドは *vlan-id1* から *vlan-id2* の VLAN を作成します。

vlan all コマンドは VLAN 1～VLAN 4094 を作成します。

undo vlan コマンドは指定された VLAN を削除します。

システムデフォルト VLAN（VLAN 1）を作成あるいは削除することはできません。

例

コンフィグレーションプロファイル **ap1** に VLAN 2 を作成し、その view に移行します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 2

[AC-config-profile-ap1-vlan2]

コンフィグレーションプロファイル **ap1** に VLAN 4～VLAN 100 を作成します。

<AC> system-view

[AC] configuration profile ap1 model QX-W1030

[AC-config-profile-ap1] vlan 4 to 100

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

8.WLAN セキュリティ

本マニュアルは以下に示す章で構成されています。

01-WLAN セキュリティ

02-WIPS

目次

このセクションのページは **8-x-x** です。

1 章 WLAN セキュリティ 1-1
1.1 WLAN セキュリティコマンド 1-1
1.1.1 akm mode 1-1
1.1.2 akm sae pwe 1-2
1.1.3 cipher-suite 1-3
1.1.4 enhanced-open enable 1-4
1.1.5 enhanced-open transition-mode service-template 1-5
1.1.6 gtk-rekey client-offline enable 1-6
1.1.7 gtk-rekey enable 1-7
1.1.8 gtk-rekey method 1-7
1.1.9 key-derivation 1-9
1.1.10 pmf 1-10
1.1.11 pmf association-comeback 1-11
1.1.12 pmf saquery retrycount 1-11
1.1.13 pmf saquery retrytimeout 1-12
1.1.14 preshared-key 1-13
1.1.15 ptk-lifetime 1-14
1.1.16 ptk-rekey enable 1-15
1.1.17 security-ie 1-16
1.1.18 snmp-agent trap enable wlan usersec 1-17
1.1.19 tkip-cm-time 1-18
1.1.20 wep key 1-19
1.1.21 wep key-id 1-20
1.1.22 wep mode dynamic 1-21
1.1.23 wpa3 1-22

1章 WLAN セキュリティ

1.1 WLANセキュリティコマンド

1.1.1 akm mode

Syntax

akm mode { **dot1x** | **psk** }

undo akm mode

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

dot1x: 802.1X を指定します。

psk: PSK を指定します。

説明

akm mode コマンドは AKM（Authentication and Key Management）モードを設定します。

undo akm mode コマンドはデフォルトに戻します。

RSNA ネットワークに AKM モードを設定する必要があります。

WLAN サービステンプレートは AKM モードを 1 つだけサポートします。WLAN サービステンプレートが無効なときだけ AKM モードを設定します。

OSEN IE モデルが使用される場合、ワイファイアライアンス Anonymous 802.1X AKM を設定します。

以下の AKM モードは、いずれも特定の認証モードで使用する必要があります。

- 802.1X AKM—802.1X 認証モード
- PSK AKM—MAC もしくはバイパス認証モード

詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“を参照してください。

例

PSK AKM モードを設定します。

<Sysname> system-view

[Sysname] wlan service-template security

[Sysname-wlan-st-security] akm mode psk

関連コマンド

- **cipher-suite**
- **security-ie**

1.1.2 akm sae pwe

Syntax

akm sae pwe { both-h2e-hnp | h2e | hnp }

undo akm sae pwe

デフォルト

H2E もしくは HnP

View

Service template view

定義済みユーザロール

network-admin

パラメータ

both-h2e-hnp:H2E 方式と HnP 方式の両方のサポートを指定します。

h2e:H2E 方式を指定します。

hnp:HnP 方式を指定します。

説明

WPA3-SAE 相互作用プロセスの PWE 導出方法を指定するには、**akm sae pwe** を使用します。

デフォルトに戻すには、**undo akm sae pwe** を使用します。

Hash - to - Element (H2E) は、 WPA3 の SAE プロセスにおいて PWE を生成するための新しい方法であり、従来の HnP (Hunting - and - Pecking) 法に比べて高いセキュリティを有します。

PWE を生成する特定の方法は、クライアント自身によって決定されます。特定の派生 PWE 方式のみが設定されている場合、この方式をサポートしていない端末は無線ネット

ワークに接続できません。端末との互換性を高めるためのベストプラクティスとして、両方の h2e-hnp 方式を指定します。

例

H2E を使用するように装置に設定します。

<Sysname> system-view

[Sysname] wlan service-template 1

[Sysname-wlan-st-1] akm sae pwe h2e

関連コマンド

- **wpa3**

1.1.3 cipher-suite

Syntax

cipher-suite { **ccmp** | **gcmp** | **tkip** | **wep40** | **wep104** | **wep128** }

undo cipher-suite { **ccmp** | **gcmp** | **tkip** | **wep40** | **wep104** | **wep128** }

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

ccmp: AES-CCMP 暗号方式を指定します。

gcmp: AES-GCMP 暗号方式を指定します。

tkip: TKIP 暗号方式を指定します。

wep40: WEP40 暗号方式を指定します。

wep104: WEP104 暗号方式を指定します。

wep128: WEP128 暗号方式を指定します。

説明

cipher-suite コマンドはフレーム暗号化に使用する暗号方式を指定します。

undo cipher-suite コマンドは指定した暗号方式を無効にします。

802.11 i ネットワーク用の cipher スイートを設定する必要があります。WLAN サービステンプレートが無効の場合にのみ cipher スイートを設定します。

RSN IE あるいは WPA IE を設定するとき、TKIP、CCMP、あるいは GCMP 暗号方式を設定します。

WEP 暗号方式には、WEP40、WEP104、WEP128 の 3 タイプ含まれます。各 WLAN サービステンプレートは WEP 暗号方式の 1 タイプのみをサポートします。WEP 暗号方式のタイプを設定したあと、タイプの同じ鍵を作成および適用しなければなりません。

CCMP、TKIP あるいは GCMP 暗号方式が設定されている場合、WEP128 は設定できません。

例

フレーム暗号化用の TKIP 暗号方式を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] cipher-suite tkip

関連コマンド

- **security-ie**

1.1.4 enhanced-open enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.6.08c を含む以降のソフトウェアでサポートしています。

Syntax

enhanced-open enable

undo enhanced-open enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

enhanced-open enable コマンドは Enhanced Open システム認証を有効にします。

undo enhanced-open enable コマンドは Enhanced Open システム認証を無効にします。

例

Enhanced Open システム認証を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] enhanced-open enable

関連コマンド

enhanced-open transition-mode service-template

1.1.5 enhanced-open transition-mode service-template

🕮 **メモ**:

このコマンドはソフトウェアバージョン 9.6.08c を含む以降のソフトウェアでサポートしています。

Syntax

enhanced-open transition-mode service-template *service-template-name*

undo enhanced-open transition-mode service-template

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

service-template-name: 大文字と小文字を区別しない 1～63 文字の文字列でサービステンプレートの名前を指定します。

説明

enhanced-open transition-mode service-template コマンドは移行モードでの推奨サービステンプレートを指定します。

undo enhanced-open transition-mode service-template コマンドはデフォルト設定に戻します。

このコマンドを複数回実行した場合、最後に実行した設定が反映されます。

例

サービステンプレート **service1** に対して、移行モードでの推奨サービステンプレートとして **service2** を指定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] enhanced-open transition-mode service-template service2

関連コマンド

- **beacon ssid-hide**
- **enhanced-open enable**

1.1.6 gtk-rekey client-offline enable

Syntax

gtk-rekey client-offline enable

undo gtk-rekey client-offline enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

gtk-rekey client-offline enable コマンドは offline-triggered GTK update を有効にします。

undo gtk-rekey client-offline コマンドはデフォルトに戻します。

GTK update が有効な場合のみ offline-triggered GTK update を有効にします。

例

offline-triggered GTK update を有効にします。

<Sysname> system-view

[Sysname] wlan service-template security

[Sysname-wlan-st-security] gtk-rekey client-offline enable

関連コマンド

- **gtk-rekey enable**

1.1.7 gtk-rekey enable

Syntax

gtk-rekey enable

undo gtk-rekey enable

デフォルト

有効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

gtk-rekey enable コマンドは GTK update を有効にします。

undo gtk-rekey enable コマンドは GTK update を無効にします。

例

GTK update を有効にします。

<Sysname> system-view

[Sysname] wlan service-template security

[Sysname-wlan-st-security] gtk-rekey enable

1.1.8 gtk-rekey method

Syntax

gtk-rekey method { **packet-based** [*packet*] | **time-based** [*time*] }

undo gtk-rekey method

デフォルト

GTK は 86400 秒間隔でアップデートされます。

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

packet-based *packet*: GTK がアップデートされる前に、マルチキャストとブロードキャストを含む伝送パケットの数を指定します。packet 引数の値の範囲は 5000~4294967295 です。

time-based *time*: GTK がアップデートされる間隔を指定します。time 引数の値の範囲は 180~604800 秒であり、デフォルトは 86400 秒です。

説明

gtk-rekey method コマンドは GTK update 手法を設定します。

undo gtk-rekey method コマンドはデフォルトに戻します。

GTK update が有効な場合のみ GTK update 手法を設定します。

直近のコンフィグレーションは、それ以前のコンフィグレーションを上書きします。例えば、packet に基づく手法を設定した後 time に基づく設定をする場合、time に基づく手法が効力をもちます。

サービステンプレートが有効になった後 GTK update 手法を設定する場合、以下の条件が存在するとき変更点が反映されます。

- GTK update 間隔を変更する場合、すでに設定されていたタイマが終了したとき新たな間隔が反映されます。
- パケット数のしきい値を変更する場合、新たなしきい値は即座に反映されます。
- GTK update 手法を packet ベースに変更する場合、タイマが消去されパケット数がしきい値に達したとき新たな設定が反映されます。
- GTK update 手法を時間ベースに変更する場合、新たな設定は即座に反映されます。

例

アップデート間隔に基づく GTK update を有効にします。

<Sysname> system-view

[Sysname] wlan service-template security

[Sysname-wlan-st-security] gtk-rekey method time-based 3600

パケットに基づく GTK update を有効にします。

<Sysname> system-view

[Sysname] wlan service-template security

[Sysname-wlan-st-security] gtk-rekey method packet-based 600000

関連コマンド

- **gtk-rekey enable**

1.1.9 key-derivation

Syntax

key-derivation { **sha1** | **sha1-and-sha256** | **sha256** }

undo key-derivation

デフォルト

sha1

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

sha1: HMAC-SHA1 アルゴリズムを KDF として指定します。

sha256: HMAC-SHA256 アルゴリズムを KDF として指定します。

sha1-and-sha256: HMAC-SHA1 アルゴリズムと HMAC-SHA256 アルゴリズムを KDF として指定します。

説明

key-derivation コマンドは KDF（Key Derivation Function）を設定します。

undo key-derivation コマンドはデフォルトに戻します。

KDF は、RSNA メカニズムを使用するネットワークに対してのみ有効です。

管理フレーム保護が有効になっている場合、HMAC-SHA256 アルゴリズムを KDF として構成することをお勧めします。

例

HMAC-SHA256 アルゴリズムを KDF として構成します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] key-derivation sha256

関連コマンド

- **akm mode**
- **cipher-suite**

- **security-ie**

1.1.10 pmf

Syntax

pmf { **mandatory** | **optional** }

undo pmf

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

mandatory: 必須モードを指定します。管理フレーム保護をサポートしたクライアントのみ WLAN にアクセスできます。

optional: オプションモードを指定します。すべてのクライアントが WLAN にアクセスできます。

説明

pmf コマンドは管理フレーム保護を有効にします。

undo pmf コマンドはデフォルトに戻します。

管理フレーム保護は、暗号化規格が RSN かつ暗号化方式が CCMP である RSNA メカニズムを使用するネットワークにのみ適用されます。

例

オプションモードで管理フレーム保護を有効にします。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf optional

関連コマンド

- **security-ie**
- **cipher-suite**

1.1.11 pmf association-comeback

Syntax

pmf association-comeback *time*

undo pmf association-comeback

デフォルト

1 秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: association comeback time を指定します。設定範囲は 1~20 秒です。

説明

pmf association-comeback コマンドは association comeback time を設定します。

undo pmf association-comeback コマンドはデフォルトに戻します。

AP がクライアントからの現在のアソシエーションまたは再アソシエーション要求を拒否した場合、アソシエーション復帰時間を含むアソシエーション/再アソシエーション応答を返します。アソシエーションカムバックタイムアウトが発生すると、AP はクライアントからのアソシエーションまたは再アソシエーション要求の受信を開始します。

例

association comeback time を 2 秒に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf association-comeback 2

1.1.12 pmf saquery retrycount

Syntax

pmf saquery retrycount *count*

undo pmf saquery retrycount

デフォルト

4 回

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

count: SA クエリ要求の最大試行回数を指定します。設定範囲は 1~16 です。

説明

pmf saquery retrycount コマンドは SA クエリ要求を再伝送する試行回数を最大にします。

undo pmf saquery retrycount コマンドはデフォルトに戻します。

最大試行回数に達した後 AP が SA クエリ要求への確認を受信しない場合、AP はクライアントをオフラインにします。

例

SA クエリ要求への最大試行回数を 3 に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf saquery retrycount 3

関連コマンド

- **pmf**
- **pmf saquery retrycount**

1.1.13 pmf saquery retrytimeout

Syntax

pmf saquery retrytimeout *timeout*

undo pmf saquery retrytimeout

デフォルト

200 ミリ秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

timeout: AP が SA クエリ要求を送信する間隔を指定します。設定範囲は 100~500 ミリ秒です。

説明

pmf saquery retrytimeout コマンドは SA クエリ要求を送信する間隔を設定します。

undo pmf saquery retrytimeout コマンドはデフォルトに戻します。

例

SA クエリ要求を送信する間隔を 300 ミリ秒に設定します。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] pmf saquery retrytimeout 300

関連コマンド

- **pmf**
- **pmf saquery retrytimeout**

1.1.14 preshared-key

🕮 **メモ：**

ソフトウェアバージョン 9.4.13 を含む以降のソフトウェアから、**pass-phrase** 文字列で ”?” の文字の使用をサポートしています。
下記以外の文字は使用可能です。

- ダブルクォーテーション
- タブ
- キャリッジリターン

Syntax

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

pass-phrase: 1~16 の範囲で SA クエリ要求の最大試行回数を指定します。

raw-key: 文字列で PSK を設定します。

cipher: 16 進数で PSK を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、プレーンテキストで指定された鍵は暗号化された形式で保存されます。

string: 鍵の文字列を指定します。この引数は大文字、小文字を区別します。鍵長は鍵タイプにより変わります。

- pass-phrase(プレーンテキスト)－8~63 文字
- pass-phrase(暗号テキスト)－8~117 文字
- raw-key(プレーンテキスト)－16 進数で 64 桁
- raw-key(暗号テキスト)－8~117 文字

説明

preshared-key コマンドは PSK を設定します。

undo preshared-key コマンドはデフォルトに戻します。

WLAN サービステンプレートが無効で、AKM モードが PSK のときにのみ PSK を設定します。AKM モードが 802.1X のときに PSK を設定した場合、WLAN サービステンプレートは有効ですが PSK コンフィグレーションは反映されません。

WLAN サービステンプレートに設定できる PSK は 1 つだけです

例

PSK としてプレーンテキストで文字列 12345678 を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] akm mode psk

[AC-wlan-st-security] preshared-key pass-phrase simple 12345678

関連コマンド

- **akm mode**

1.1.15 ptk-lifetime

Syntax

ptk-lifetime *time*

undo ptk-lifetime

デフォルト

43200 秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: PSK ライフタイムを指定します。設定範囲は 180~604800 秒です。

説明

ptk-lifetime コマンドは PKT ライフタイムを設定します。

undo ptk-lifetime コマンドはデフォルトに戻します。

サービステンプレートが有効なときに PTK ライフタイムを設定する場合、その設定は既定のタイマが終了した後に反映されます。

例

PTK ライフタイムを 200 秒に設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] ptk-lifetime 200

1.1.16 ptk-rekey enable

Syntax

ptk-rekey enable

undo ptk-rekey enable

デフォルト

有効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

ptk-rekey enable コマンドは PTK 更新を有効にします。

undo ptk-rekey enable コマンドは PTK 更新を無効にします。

この機能により、設定された PTK の有効期限が切れた後、装置は PTK を更新できます。

例

PTK 更新を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] ptk-rekey enable

関連コマンド

- **ptk-lifetime**

1.1.17 security-ie

Syntax

security-ie { **rsn** | **wpa** }

undo security-ie { **rsn** | **wpa** }

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

rsn: AP から送信されたビーコンおよびプローブ応答フレーム内の RSN IE を有効にします。RSN IE は、AP の RSN 機能をアドバタイズします。

wpa: AP から送信されたビーコンおよびプローブ応答フレーム内の WPA IE を有効にします。WPA IE は、AP の WPA 機能をアドバタイズします。

説明

security-ie コマンドはビーコンおよびプローブ要求内で OSEN IE、RSN IE、あるいは WPA IE を有効にします。

undo security-ie コマンドはビーコンおよびプローブ要求内で OSEN IE、RSN IE、あるいは WPA IE を無効にします。

802.11 i ネットワークのセキュリティ IE を設定する必要があります。セキュリティ IE は、WLAN サービステンプレートが無効で、CCMP または TKIP cipher スイートが設定されている場合にのみ設定してください。

OSEN IE を使用する場合は、WiFi アライアンスの匿名 802.1 X AKM モードを設定します。

例

ビーコンおよびプローブ応答で RSN IE をイネーブルにします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] security-ie rsn

関連コマンド

- **akm mode**
- **cipher-suite**

1.1.18 snmp-agent trap enable wlan usersec

Syntax

snmp-agent trap enable wlan usersec

undo snmp-agent trap enable wlan usersec

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan usersec コマンドは WLAN セキュリティに対して SNMP 通知を有効にします。

undo snmp-agent trap enable wlan usersec コマンドは WLAN セキュリティに対して SNMP 通知を無効にします

重要な WLAN セキュリティイベントを NMS に報告するために、WLAN セキュリティに対して SNMP 通知を有効にします。

例

WLAN セキュリティに対して SNMP 通知を有効にします。

<AC> system-view

[AC] snmp-agent trap enable wlan usersec

1.1.19 tkip-cm-time

Syntax

tkip-cm-time *time*

undo tkip-cm-time

デフォルト

0 秒

AP は対策をとりません。

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: TKIP MIC 障害ホールド時間を設定します。設定範囲は 0~3600 秒です。

説明

tkip-cm-time コマンドは TKIP MIC 失敗ホールド時間を設定します。

undo tkip-cm-time コマンドはデフォルトに戻します。

暗号化方式に TKIP が設定されているときにのみ TKIP MIC 障害ホールド時間を設定します。

サービステンプレートが有効なときに MIC 障害ホールド時間を設定する場合、その設定は既定のタイマが終了したあとに反映されます。

MIC 障害ホールド時間内に AP が 2 つの MIC 障害を検出した場合、AP はすべてのクライアントを 60 秒間分離させます。

例

TKIP MIC 障害ホールド時間を 180 秒に設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] tkip-cm-time 180

関連コマンド

- **cipher-suite**

1.1.20 wep key

Syntax

wep key *key-id* { **wep40** | **wep104** | **wep128** } { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo wep key *key-id*

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

key-id: key ID を設定します。設定範囲は 1~4 です。

wep40: WEP40 key を設定します。

wep104: WEP104 key を設定します。

wep128: WEP128 key を設定します。

pass-phrase: WEP key を文字列で設定します。

raw-key: WEP key を 16 進数で設定します。

cipher: 暗号テキストで鍵を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、平文形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵列を指定します。大文字と小文字を区別します。設定範囲は 37~73 文字です。プレーンテキストの鍵の長さは鍵タイプにより異なります。

- wep40 pass-phrase(プレーンテキスト)－5 文字
- wep104 pass-phrase(プレーンテキスト)－13 文字
- wep128 pass-phrase(プレーンテキスト)－16 文字
- wep40 raw-key(プレーンテキスト)－16 進数で 10 桁
- wep104 raw-key(プレーンテキスト)－16 進数で 26 桁
- wep128 raw-key(プレーンテキスト)－16 進数で 32 桁

説明

wep key コマンドは WEP key を設定します。

undo wep key コマンドは設定した WEP key を削除します。

WLAN サービステンプレートが無効で、暗号化方式に WEP が設定されているときにのみ WEP key を設定します。最大で 4 つの WEP key を設定できます。

例

暗号化方式に WEP40 を設定し、WEP key 1 としてプレーンテキスト 12345 を設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] cipher-suite wep40

[AC-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345

関連コマンド

- **cipher-suite**
- **wep key-id**

1.1.21 wep key-id

Syntax

wep key-id { **1** | **2** | **3** | **4** }

undo wep key-id

デフォルト

Key1

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

1: ID が 1 の WEP key を指定します。

2: ID が 2 の WEP key を指定します。

3: ID が 3 の WEP key を指定します。

4: ID が 4 の WEP key を指定します。

説明

wep key-id コマンドは WEP key を適用します。

undo wep key-id コマンドはデフォルトに戻します。

WLAN サービステンプレートが無効の場合にのみ WEP キーを適用します。

802.11 i メカニズムでは、キー 1 はネゴシエートされた鍵です。WEP キーを適用するには、ID が 1 以外の WEP キーを指定します。

既存の WEP キーのみ適用できます。

例

暗号化方式に WEP40 を設定し、WEP key 1 としてプレーンテキスト 12345 を設定し、WEP key 1 を適用します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] cipher-suite wep40

[AC-wlan-st-security] wep key 1 wep40 pass-phrase simple 12345

[AC-wlan-st-security] wep key-id 1

関連コマンド

- **wep key**

1.1.22 wep mode dynamic

Syntax

wep mode dynamic

undo wep mode dynamic

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

wep mode dynamic コマンドはダイナミック WEP メカニズムを有効にします。

undo wep mode dynamic コマンドはダイナミック WEP メカニズムを無効にします。

WLAN サービステンプレートが無効のときのみ WEP メカニズムを有効にします。

ダイナミック WEP メカニズムはユーザアクセス認証のために 802.1X 認証を要求します。

ダイナミック WEP メカニズムが有効な場合、WEP key 4 を適用しないでください。

例

ダイナミック WEP メカニズムを有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] wep mode dynamic

関連コマンド

- **cipher-suite**
- **client-security authentication-mode**
- **wep key**
- **wep key-id**

1.1.23 wpa3

🕮 **メモ**:

wpa3 enterprise-only-mode と **wpa3 enterprise-transition-mode** を設定する場合、事前に **pmf** コマンドと **key-derivation** コマンドがサービステンプレートに設定されていないことを確認してください。

Syntax

wpa3 { **enterprise** | | **enterprise-only-mode** | **enterprise-transition-mode** | **personal** { **mandatory** | **optional** } }

undo wpa3

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

mdc-admin

パラメータ

enterprise: WPA3 エンタープライズの 192bit セキュリティモードを使用します。

enterprise-only-mode: WPA3 エンタープライズで WPA3 セキュリティモードを必須モードに指定します。WPA3 セキュリティモードをサポートしていないクライアントはア

クセスできません。このパラメータを指定した場合、**pmf mandatory**、**key-derivation sha256** を設定したときと同じ動作となります。

enterprise-transition-mode: WPA3 エンタープライズで WPA3 セキュリティモードを WPA3 移行モードに指定します。このモードでは、WPA3 セキュリティモードをサポートしているクライアントとサポートしていないクライアントのどちらもアクセスできます。このパラメータを指定した場合、**pmf optional**、**key-derivation sha1-and-sha256** を設定したときと同じ動作となります。

personal: WPA3 パーソナルを使用します。

mandatory: WPA3 パーソナルで WPA3 セキュリティモードを必須モードに指定します。WPA3 セキュリティモードをサポートしていないクライアントはアクセスできません。

optional: WPA3 パーソナルで WPA3 セキュリティモードをオプションモードに指定します。WPA3 セキュリティモードをサポートしているクライアントとサポートしていないクライアントのどちらもアクセスできます。

説明

wpa3 コマンドは WPA3 エンタープライズの 192bit セキュリティモード、または、WPA3 パーソナルを有効にします。

undo wpa3 コマンドは WPA3 エンタープライズの 192bit セキュリティモード、または、

WPA 3-Enterprise を使用するには、cipher スイートを GCMP、セキュリティ IE を RSN に設定します。

WPA 3-SAE を使用するには、cipher スイートを CCMP、セキュリティ IE を RSN に設定します。

WPA 3 セキュリティモードを指定する場合は、管理フレーム保護を有効にすることをお勧めします。

WPA 3 セキュリティモードを設定しないで、802.11 r FT または拡張オープンシステム認証を同時に有効にします。この場合、サービステンプレートを有効にできません。802.11 r の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*10 WLAN ローミング*”を参照してください。

例

WPA3 セキュリティモードをパーソナルレベルの必須モードに設定します。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] wpa3 personal mandatory

関連コマンド

- **cipher-suite**
- **security-ie**

目次

このセクションのページは **8-x-x** です。

2 章 WIPS 2-1
2.1 WIPS 設定コマンド 2-1
2.1.1 ap-channel-change 2-1
2.1.2 ap-classification rule 2-2
2.1.3 ap-flood 2-2
2.1.4 ap-impersonation 2-3
2.1.5 apply ap-classification rule 2-4
2.1.6 apply classification policy 2-5
2.1.7 apply countermeasure policy 2-6
2.1.8 apply detect policy 2-7
2.1.9 apply signature policy 2-7
2.1.10 apply signature rule 2-8
2.1.11 ap-rate-limit 2-9
2.1.12 ap-spoofing 2-10
2.1.13 ap-timer 2-11
2.1.14 association-table-overflow 2-12
2.1.15 authentication 2-13
2.1.16 block mac-address 2-14
2.1.17 classification policy 2-15
2.1.18 client-online 2-15
2.1.19 client-rate-limit 2-16
2.1.20 client-spoofing 2-17
2.1.21 client-timer 2-18
2.1.22 countermeasure adhoc 2-19
2.1.23 countermeasure attack all 2-20
2.1.24 countermeasure attack deauth-broadcast 2-21
2.1.25 countermeasure attack disassoc-broadcast 2-21
2.1.26 countermeasure attack honeypot-ap 2-22
2.1.27 countermeasure attack hotspot-attack 2-23
2.1.28 countermeasure attack ht-40-mhz-intolerance 2-23
2.1.29 countermeasure attack malformed-packet 2-24
2.1.30 countermeasure attack man-in-the-middle 2-25
2.1.31 countermeasure attack omerta 2-25
2.1.32 countermeasure attack power-save 2-26
2.1.33 countermeasure attack soft-ap 2-27
2.1.34 countermeasure attack unencrypted-trust-client 2-27

2.1.35 countermeasure attack weak-iv 2-28
2.1.36 countermeasure attack windows-bridge 2-29
2.1.37 countermeasure external-ap 2-29
2.1.38 countermeasure mac-address 2-30
2.1.39 countermeasure misassociation-client 2-31
2.1.40 countermeasure misconfigured-ap 2-32
2.1.41 countermeasure policy 2-32
2.1.42 countermeasure potential-authorized-ap 2-33
2.1.43 countermeasure potential-external-ap 2-34
2.1.44 countermeasure potential-rogue-ap 2-34
2.1.45 countermeasure rogue-ap 2-35
2.1.46 countermeasure unauthorized-client 2-36
2.1.47 countermeasure uncategorized-ap 2-36
2.1.48 countermeasure uncategorized-client 2-37
2.1.49 deauthentication-broadcast 2-38
2.1.50 detect dissociate-client enable 2-39
2.1.51 detect policy 2-39
2.1.52 detect signature 2-40
2.1.53 disassociation-broadcast 2-41
2.1.54 discovered-ap 2-42
2.1.55 display wips sensor 2-43
2.1.56 display wips statistics 2-44
2.1.57 display wips virtual-security-domain countermeasure record 2-49
2.1.58 display wips virtual-security-domain device 2-50
2.1.59 display wlan nat-detect 2-57
2.1.60 flood association-request 2-58
2.1.61 flood authentication 2-59
2.1.62 flood beacon 2-60
2.1.63 flood block-ack 2-61
2.1.64 flood cts 2-62
2.1.65 flood deauthentication 2-63
2.1.66 flood disassociation 2-64
2.1.67 flood eap-failure 2-65
2.1.68 flood eapol-logoff 2-66
2.1.69 flood eapol-start 2-67
2.1.70 flood eap-success 2-68
2.1.71 flood null-data 2-69
2.1.72 flood probe-request 2-70
2.1.73 flood reassociation-request 2-71
2.1.74 flood rts 2-72
2.1.75 frame-type 2-73
2.1.76 honeypot-ap 2-74
2.1.77 hotspot-attack 2-75

2.1.78 ht-40mhz-intolerance 2-76
2.1.79 ht-greenfield 2-77
2.1.80 ignorelist 2-78
2.1.81 import hotspot 2-79
2.1.82 import oui 2-79
2.1.83 invalid-oui-classify illegal 2-80
2.1.84 mac-address 2-81
2.1.85 malformed duplicated-ie 2-82
2.1.86 malformed fata-jack 2-83
2.1.87 malformed illegal-ibss-ess 2-84
2.1.88 malformed invalid-address-combination 2-85
2.1.89 malformed invalid-assoc-req 2-86
2.1.90 malformed invalid-auth 2-87
2.1.91 malformed invalid-deauth-code 2-88
2.1.92 malformed invalid-disassoc-code 2-89
2.1.93 malformed invalid-ht-ie 2-90
2.1.94 malformed invalid-ie-length 2-91
2.1.95 malformed invalid-pkt-length 2-91
2.1.96 malformed large-duration 2-92
2.1.97 malformed null-probe-resp 2-93
2.1.98 malformed overflow-eapol-key 2-94
2.1.99 malformed overflow-ssid 2-95
2.1.100 malformed redundant-ie 2-96
2.1.101 man-in-the-middle 2-97
2.1.102 manual-classify mac-address 2-98
2.1.103 match all (AP classification rule view) 2-99
2.1.104 match all (signature view) 2-99
2.1.105 omerta 2-100
2.1.106 oui 2-101
2.1.107 pattern 2-102
2.1.108 permit-channel 2-103
2.1.109 power-save 2-104
2.1.110 prohibited-channel 2-105
2.1.111 random-mac-scan 2-106
2.1.112 report-interval 2-107
2.1.113 reset wips statistics 2-108
2.1.114 reset wips virtual-security-domain 2-108
2.1.115 reset wips virtual-security-domain countermeasure record 2-109
2.1.116 reset wlan nat-detect 2-110
2.1.117 rssi 2-110
2.1.118 rssi-change-threshold 2-111
2.1.119 rssi-threshold 2-112
2.1.120 security 2-112

2.1.121 select sensor all 2-113
2.1.122 seq-number 2-114
2.1.123 signature policy 2-115
2.1.124 signature rule 2-116
2.1.125 soft-ap 2-116
2.1.126 ssid (AP classification rule view) 2-117
2.1.127 ssid (signature view) 2-118
2.1.128 ssid-length 2-119
2.1.129 trust mac-address 2-120
2.1.130 trust oui 2-121
2.1.131 trust ssid 2-122
2.1.132 unencrypted-authorized-ap 2-122
2.1.133 unencrypted-trust-client 2-123
2.1.134 up-duration 2-124
2.1.135 virtual-security-domain 2-125
2.1.136 weak-iv 2-126
2.1.137 windows-bridge 2-127
2.1.138 wips (system view) 2-127
2.1.139 wips enable 2-128
2.1.140 wips virtual-security-domain 2-129
2.1.141 wireless-bridge 2-130
2.1.142 wlan nat-detect 2-131

2章 WIPS

2.1 WIPS設定コマンド

2.1.1 ap-channel-change

Syntax

ap-channel-change [**quiet** *quiet-value*]

undo ap-channel-change

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*:チャネル変更時に WIPS がアラームをトリガーしてからの待機時間を指定します。quiet-value 引数の値の範囲は 5~604800 秒で、デフォルトの待機時間は 600 秒です。WIPS は、待機時間内にチャネル変更を検出してもアラームをトリガーしません。

説明

ap-channel-change コマンドはチャネル変更検出を設定します。

undo ap-channel-change コマンドはチャネル変更検出を無効にします。

例

チャネル変更検出を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] ap-channel-change quiet 5

2.1.2 ap-classification rule

Syntax

ap-classification rule *rule-id*

undo ap-classification rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザーロール

network-admin

パラメータ

rule-id: ID で AP 分類ルールを指定します。値の範囲は 1～65535 です。

説明

ap-classification rule コマンドは AP 分類ルールを作成し、その view に移行します。AP 分類ルールがすでに存在する場合、ap-classification rule コマンドで AP classification rule view に移行します。

undo ap-classification rule コマンドは AP 分類ルールを削除します。

例

AP classification rule 1 を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

2.1.3 ap-flood

Syntax

ap-flood [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *

undo ap-flood

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

apnum *apnum-value*: AP 番号のしきい値を指定します。値の範囲は 10～200 です。デフォルト値は 80 です。

exceed *exceed-value*: 許容される超過 AP の最大数を指定します。exceed-value 引数の値の範囲は 10～200 です。デフォルト値は 80 です。AP の数が、AP 番号のしきい値と、超過を許可された AP の最大数の合計を超える場合、WIPS は AP フラッド攻撃アラームを引き起こします。

quiet *quiet-value*: WIPS が AP フラッド攻撃アラームを引き起こした後、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP フラッド攻撃を検出してもアラームを引き起こしません。

説明

ap-flood コマンドは AP フラッド攻撃検出を設定します。

undo ap-flood コマンドは AP フラッド攻撃検出を無効にします。

例

AP フラッド攻撃検出を有効にし、apnum-value、exceed-value、quiet-value をそれぞれ 50、50、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-flood apnum 50 exceed 50 quiet 100

2.1.4 ap-impersonation

Syntax

ap-impersonation [**quiet** *quiet-value*]

undo ap-impersonation

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP なりすまし攻撃アラームを引き起こした後、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP なりすまし攻撃を検出してもアラームを引き起こしません。

説明

ap-impersonation コマンドは AP なりすまし攻撃検出を設定します。

undo ap-impersonation コマンドはデフォルトに戻します。

例

AP なりすまし攻撃検出を有効にし、遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-impersonation quiet 360

2.1.5 apply ap-classification rule

Syntax

apply ap-classification rule *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }

undo apply ap-classification rule *rule-id*

デフォルト

設定なし

View

Classification view

定義済みユーザーロール

network-admin

パラメータ

*rule-id:*AP 分類ルールを ID で 1 から 65535 の範囲で指定します。

authorized-ap:AP 分類ルールに一致する AP を許可 AP として指定します。

external-ap:AP 分類ルールに一致する AP を外部 AP として指定します。

misconfigured-ap:AP 分類ルールに一致する AP を誤設定 AP として指定します。

rogue-ap:AP 分類ルールに一致する AP を不正 AP として指定します。

level:AP 分類ルールに一致する AP の重大度を 1 から 100 の範囲で指定します。デフォルトの重大度は 50 です。

説明

apply ap-classification rule コマンドを使用して、AP 分類ルールを分類ポリシーに適用します。

undo apply ap-classification rule コマンドを使用して、適用された AP 分類ルールを削除します。

例

ID 1 の AP 分類ルールを home という名前の分類ポリシーに適用し、AP を違法 AP として分類、リスクレベルを 80 に定義します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] classification policy home

[Sysname-wips-cls-home] apply ap-classification rule 1 rogue-ap severity-level 80

関連コマンド

- **ap-classification rule**

2.1.6 apply classification policy

Syntax

apply classification policy *policy-name*

undo apply classification policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザーロール

network-admin

パラメータ

policy-name:分類ポリシー名。1~63 文字の文字列で、大文字と小文字が区別されます。

説明

apply classification policy コマンドを使用して、分類ポリシーを VSD に適用します。

undo apply classification policy コマンドを使用して、適用された分類ポリシーを削除します。

例

#分類ポリシーpolicy1 を VSD に適用します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] virtual-security-domain home

[Sysname-wips-vsd-home] apply classification policy policy1

2.1.7 apply countermeasure policy

Syntax

apply countermeasure policy *policy-name*

undo apply countermeasure policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザーロール

network-admin

パラメータ

policy-name:ポリシー名を 1~63 文字の文字列として反転します。大文字と小文字が区別されます。

説明

apply countermeasure policy コマンドを使用して、VSD にリバースポリシーを適用します。

undo apply countermeasure policy コマンドを使用して、適用されたリバースポリシーを削除します。

例

#VSD にリバースポリシーpolicy2 を適用します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] virtual-security-domain home

[Sysname-wips-vsd-home] apply countermeasure policy policy2

2.1.8 apply detect policy

Syntax

apply detect policy *policy-name*

undo apply detect policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザーロール

network-admin

パラメータ

policy-name:攻撃検出ポリシー名。1~63 文字の文字列で、大文字と小文字が区別されます。

説明

apply detect policy コマンドは、VSD に攻撃検出ポリシーを適用するために使用されます。

undo apply detect policy コマンドを使用して、適用された攻撃検出ポリシーを削除します。

例

#VSD に攻撃検知ポリシーpolicy2 を適用します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] virtual-security-domain home

[Sysname-wips-vsd-home] apply detect policy policy2

2.1.9 apply signature policy

Syntax

apply signature policy *policy-name*

undo apply signature policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザーロール

network-admin

パラメータ

policy-name:Signature ポリシーの名前。1~63 文字の文字列で、大文字と小文字が区別されます。

説明

apply signature policy コマンドは、VSD 内で Signature ポリシーを適用するために使用されます。

undo apply signature policy コマンドを使用して、適用された Signature ポリシーを削除します。

例

#policy1 という名前の Signature ポリシーを home という名前の VSD に適用します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] virtual-security-domain home

[Sysname-wips-vsd-home] apply signature policy1

2.1.10 apply signature rule

Syntax

apply signature rule *rule-id*

undo apply signature rule *rule-id*

デフォルト

設定なし

View

Signature policy view

定義済みユーザーロール

network-admin

パラメータ

rule-id:ルールのルール番号値。範囲は 1~128 です。

説明

apply signature rule コマンドは、Signature ポリシーに Signature ルールを適用するために使用します。

undo apply signature rule コマンドを使用して、適用された Signature ルールを削除します。

例

Signature ポリシーoffice で ID 1 の Signature ルールを適用します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature policy office

[Sysname-wips-sig-office] apply signature rule 1

2.1.11 ap-rate-limit

Syntax

ap-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo ap-rate-limit

デフォルト

学習した AP エントリのための統計情報収集間隔：60 秒

遅延時間：1200 秒

AP エントリしきい値：512

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: 学習した AP エントリのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS が AP エントリ攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold *threshold-value*: AP エントリ攻撃アラームを引き起こす AP エントリ数を指定します。threshold-value 引数の値の範囲は 1～4096 です。

説明

ap-rate-limit コマンドは AP エントリの学習を制限します。

undo ap-rate-limit コマンドはデフォルトに戻します。

例

AP エントリの学習を制限します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-rate-limit interval 60 quiet 1600 threshold 100

関連コマンド

- **ap-timer**

2.1.12 ap-spoofing

Syntax

ap-spoofing [**quiet** *quiet-value*]

undo ap-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP スプーフィング攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こしません。

説明

ap-spoofing コマンドは AP スプーフィング攻撃を有効にします。

undo ap-spoofing コマンドは AP スプーフィング攻撃を無効にします。

この機能を有効にすると、デバイスが AP アドレスの偽装を検出すると、アラームメッセージが送信されます。

例

AP スプーフィング検出を有効にし、遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-spoofing quiet 360

2.1.13 ap-timer

Syntax

ap-timer inactive *inactive-value* **aging** *aging-value*

undo ap-timer

デフォルト

非アクティブ時間： 300 秒

エージング時間： 600 秒

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

Inactive *inactive-value* 引数の値の範囲は 1～1200 秒です。

aging *aging-value* 引数の値の範囲は 1～86400 秒です。

説明

ap-timer コマンドは AP エントリタイマを設定します。

undo ap-timer コマンドはデフォルトに戻します。

AP が指定された非アクティブ時間内にフレームを受信または送信しない場合、WIPS は AP を非アクティブ状態に設定します。AP が指定されたエージングタイム内にフレームを送受信しない場合、WIPS はエントリを削除します。

エージングタイムは、非アクティブ時間以上である必要があります。ベストプラクティスとして、デフォルトの非アクティブ時間とエージングタイムを使用します。

AP エントリの時間変化にエラーが存在する可能性があり、エラー値はセンサーが検出されたデバイスに関する情報を報告する間隔によって異なります。

例

非アクティブ時間を 120 秒、エージング時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] ap-timer inactive 120 aging 360

関連コマンド

- **ap-rate-limit**
- **report-interval**

2.1.14 association-table-overflow

Syntax

association-table-overflow [**quiet** *quiet-value*]

undo association-table-overflow

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がアソシエーション/再アソシエーション DoS 攻撃アラームを引き起こした後、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にアソシエーション/再アソシエーション DoS 攻撃を検出してもアラームを引き起こしません。

説明

association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を設定します。

undo association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を無効にします。

例

アソシエーション/再アソシエーション DoS 攻撃検出を有効にし、遅延時間を 100 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] association-table-overflow quiet 100

2.1.15 authentication

Syntax

authentication { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }

undo authentication

デフォルト

一致なし

View

AP classification rule view

定義済みユーザーロール

network-admin

パラメータ

equal: 指定された認証モードと等しい認証モードを整合します。

include: 指定された認証モードを含む認証モードを整合します。

802.1x: 802.1X 認証モードを指定します。

none: 認証モードは指定されません。

other: 802.1X と PSK 以外の認証モードを指定します。

psk: PSK 認証モードを指定します。

説明

authentication コマンドは AP の認証モードを整合するために AP 分類ルールを設定します。

undo authentication コマンドはデフォルトに戻します。

例

PSK 認証モードを使用する AP を整合するために AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] authentication equal psk

2.1.16 block mac-address

Syntax

block mac-address *mac-address*

undo block mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザーロール

network-admin

パラメータ

mac-address: AP の無線 MAC アドレス(BSSID)もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

all: すべての MAC アドレスを指定します。

説明

block mac-address コマンドはスタティック禁止装置リストに MAC アドレスを追加します。

undo block mac-address コマンドはスタティック禁止装置リストから 1 つもしくはすべての MAC アドレスを削除します。

例

スタティック禁止装置リストに MAC アドレス 78AC-C0AF-944F を追加します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home] block mac-address 78AC-C0AF-944F

2.1.17 classification policy

Syntax

lassification policy *policy-name*

undo classification policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザーロール

network-admin

パラメータ

policy-name: 分類ポリシーの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

classification policy コマンドは分類ポリシーを作成し、その view に移行します。

undo classification policy コマンドは分類ポリシーを削除します。

例

分類ポリシーhome を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] classification policy home

[AC-wips-cls-home]

2.1.18 client-online

Syntax

client-online *value1* [**to** *value2*]

undo client-online

デフォルト

一致なし

View

AP classification rule view

定義済みユーザーロール

network-admin

パラメータ

value1 to value2: AP に紐付けられたクライアント数の範囲を指定します。value1 引数と value2 引数は、それぞれ値の範囲の始めと終わりを指定します。value1 引数と value2 引数の値の範囲は、どちらも 0～128 です。ただし、value2 引数の値は value1 引数の値より大きくなければなりません。

説明

client-online コマンドは AP に関連付けられたクライアント数を整合するために AP 分類ルールを設定します。

undo client-online コマンドはデフォルトに戻します。

例

20～40 のクライアントに関連付けられた AP を整合するために、AP classification rule 1 を設定します。

<AC> system-view

[AC] wips

[AC-wips] ap-classification rule 1

[AC-wips-cls-rule-1] client-online 20 to 40

2.1.19 client-rate-limit

Syntax

client-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo client-rate-limit

デフォルト

学習したクライアントエントリのための統計情報収集間隔：60 秒

遅延時間：1200 秒

クライアントエントリしきい値：1024

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: 学習したクライアントエントリのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS がクライアントエントリ攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内にクライアントエントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold *threshold-value*: クライアントエントリ攻撃アラームを引き起こすクライアントエントリ数を指定します。threshold-value 引数の値の範囲は 1～4096 です。

説明

client-rate-limit コマンドはクライアントエントリの学習を制限します。

undo client-rate-limit コマンドはデフォルトに戻します。

例

クライアントエントリの学習を制限します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] client-rate-limit interval 80 quiet 1600 threshold 100

関連コマンド

- **client-timer**

2.1.20 client-spoofing

Syntax

client-spoofing [**quiet** *quiet-value*]

undo client-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: クライアントスプーフィング攻撃時に WIPS がアラームをトリガーしてからの待機時間を指定します。*quiet-value* 引数の値の範囲は 5~604800 秒で、デフォルトの待機時間は 600 秒です。WIPS は、待機時間内にクライアントスプーフィング攻撃を検出してもアラームをトリガーしません。

説明

client-spoofing コマンドはクライアントスプーフィング攻撃検出を有効にします。

undo client-spoofing コマンドはクライアントスプーフィング攻撃検出を無効にします。

例

クライアントスプーフィング攻撃の検出を有効にし、遅延時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] client-spoofing quiet 360

2.1.21 client-timer

Syntax

client-timer inactive *inactive-value* **aging** *aging-value*

undo client-timer

デフォルト

非アクティブ時間：300 秒

エージング時間：600 秒

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

inactive *inactive-value*: 非アクティブ時間を指定します。指定された非アクティブ時間内にクライアントがフレームを送受信しない場合、WIPS はクライアントを非アクティブ状態に設定します。

inactive-value 引数の値の範囲は 1～1200 秒です。

aging *aging-value*: エージング時間を指定します。指定されたエージング時間内にクライアントがフレームを送受信しない場合、WIPS はエントリを削除します。エージング時間は非アクティブ時間より大きくなければなりません。

aging-value 引数の値の範囲は 1～86400 秒です。

説明

client-timer コマンドはクライアントエントリタイマを設定します。

undo client-timer コマンドはデフォルトに戻します。

クライアントが指定された非アクティブ時間内にフレームを受信または送信しない場合、WIPS はクライアントを非アクティブ状態に設定します。クライアントが指定されたエージングタイム内にフレームを送受信しない場合、WIPS はエントリを削除します。

エージングタイムは、非アクティブ時間以上である必要があります。ベストプラクティスとして、デフォルトの非アクティブ時間とエージングタイムを使用します。

クライアントエントリの時間変化にエラーが存在する可能性があり、エラー値はセンサーが検出されたデバイスに関する情報を報告する間隔によって異なります。

例

非アクティブ時間を 120 秒、エージング時間を 360 秒に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] client-timer inactive 120 aging 360

関連コマンド

- **client-rate-limit**
- **report-interval**

2.1.22 countermeasure adhoc

Syntax

client-rate-limit

report-interval

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure adhoc コマンドはアドホック装置に対策を講じるために WIPS を有効にします。

undo countermeasure adhoc コマンドはデフォルトに戻します。

例

#アドホック装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure adhoc

2.1.23 countermeasure attack all

Syntax

countermeasure attack all

undo countermeasure attack all

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack all コマンドはすべての攻撃者に対して WIPS を有効にします。

undo countermeasure attack all コマンドはデフォルトに戻します。

例

#すべての攻撃者に対して WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack deauth-broadcast

2.1.24 countermeasure attack deauth-broadcast

Syntax

countermeasure attack deauth-broadcast

undo countermeasure attack deauth-broadcast

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack deauth-broadcast コマンドはブロードキャスト認証解除攻撃を開始するデバイスに対して WIPS を有効にします。

undo countermeasure attack deauth-broadcast コマンドはデフォルトに戻します。

例

ブロードキャスト認証解除攻撃を行う機器に対して、WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack deauth-broadcast

2.1.25 countermeasure attack disassoc-broadcast

Syntax

countermeasure attack disassoc-broadcast

undo countermeasure attack disassoc-broadcast

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack disassoc-broadcast コマンドはアソシエーション解除フレームをブロードキャストする装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack disassoc-broadcast コマンドはデフォルトに戻します。

例

#アソシエーション解除フレームをブロードキャストする装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack disassoc-broadcast

2.1.26 countermeasure attack honeypot-ap

Syntax

countermeasure attack honeypot-ap

undo countermeasure attack honeypot-ap

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack honeypot-ap コマンドはハニーポット AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack honeypot-ap コマンドはデフォルトに戻します。

例

ハニーポット AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack honeypot-ap

2.1.27 countermeasure attack hotspot-attack

Syntax

countermeasure attack hotspot-attack

undo countermeasure attack hotspot-attack

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack hotspot-attack コマンドはホットスポット攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack hotspot-attack コマンドはデフォルトに戻します。

例

ホットスポット攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack hotspot-attack

2.1.28 countermeasure attack ht-40-mhz-intolerance

Syntax

countermeasure attack ht-40-mhz-intolerance

undo countermeasure attack ht-40-mhz-intolerance

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack ht-40-mhz-intolerance コマンドは 40MHz 帯域幅モードが無効の装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack ht-40-mhz-intolerance コマンドはデフォルトに戻します。

例

#アドホック装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack ht-40-mhz-intolerance

2.1.29 countermeasure attack malformed-packet

Syntax

countermeasure attack malformed-packet

undo countermeasure attack malformed-packet

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack malformed-packet コマンドは不正パケットを送信する装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack malformed-packet コマンドはデフォルトに戻します。

例

不正パケットを送信する装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack malformed-packet

2.1.30 countermeasure attack man-in-the-middle

Syntax

countermeasure attack man-in-the-middle

undo countermeasure attack man-in-the-middle

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack man-in-the-middle コマンドは MITM 攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack man-in-the-middle コマンドはデフォルトに戻します。

例

MITM 攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack man-in-the-middle

2.1.31 countermeasure attack omerta

Syntax

countermeasure attack omerta

undo countermeasure attack omerta

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack omerta コマンドは Omerta 攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack omerta コマンドはデフォルトに戻します。

例

Omerta 攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack omerta

2.1.32 countermeasure attack power-save

Syntax

countermeasure attack power-save

undo countermeasure attack power-save

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack power-save コマンドはパワーセーブ攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack power-save コマンドはデフォルトに戻します。

例

パワーセーブ攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack power-save

2.1.33 countermeasure attack soft-ap

Syntax

countermeasure attack soft-ap

undo countermeasure attack soft-ap

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack soft-ap コマンドはソフト AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack soft-ap コマンドはデフォルトに戻します。

例

ソフト AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack soft-ap

2.1.34 countermeasure attack unencrypted-trust-client

Syntax

countermeasure attack unencrypted-trust-client

undo countermeasure attack unencrypted-trust-client

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack unencrypted-trust-client コマンドは暗号化されていない許可クライアントに対して対策を講じるために WIPS を有効にします。

undo countermeasure attack unencrypted-trust-client コマンドはデフォルトに戻します。

例

暗号化されていない許可されたクライアントに対してWIPSが対策できるようにする。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack unencrypted-trust-client

2.1.35 countermeasure attack weak-iv

Syntax

countermeasure attack weak-iv

undo countermeasure attack weak-iv

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack weak-iv コマンドは Weak IV を使用する装置に対策を講じるために WIPS を有効にします。

undo countermeasure attack weak-iv コマンドはデフォルトに戻します。

例

#アドホック装置に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack weak-iv

2.1.36 countermeasure attack windows-bridge

Syntax

countermeasure attack windows-bridge

undo countermeasure attack windows-bridge

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure attack windows-bridge コマンドは Windows ブリッジ攻撃に対策を講じるために WIPS を有効にします。

undo countermeasure attack windows-bridge コマンドはデフォルトに戻します。

例

Windws ブリッジ攻撃に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure attack windows-bridge

2.1.37 countermeasure external-ap

Syntax

countermeasure external-ap

undo countermeasure external-ap

デフォルト

設定なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure external-ap コマンドは、WIPS が外部 AP に対して WIPS を有効にします。

undo countermeasure external-ap コマンドを使用して、デフォルトに戻します。

例

#外部 AP に対する WIPS を有効にします。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] countermeasure policy home

[Sysname-wips-cms-home] countermeasure external-ap

2.1.38 countermeasure mac-address

Syntax

countermeasure mac-address *mac-address* [**except-authorized-ap**]

undo countermeasure mac-address { *mac-address* | **all** }

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

パラメータ

mac-address: AP の無線 MAC アドレス(BSSID)もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

except-authorized-ap:クライアントが接続している AP が許可された AP として分類されている場合、そのクライアントが手動でロールバックを指定しても、ロールバック機能は有効になりません。

all: すべての AP とクライアントを指定します。

説明

countermeasure mac-address コマンドは指定された MAC アドレスを持つ装置に対策を講じるために WIPS を有効にします。

undo countermeasure mac-address コマンドは設定を削除します。

このコマンドを複数回設定すると、WIPS が複数のデバイスに対して対策を実行できるようになります。

例

MAC アドレス 2a11-1fa1-141f を持つ装置に対策を講じるために WIPS を有効にします。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] countermeasure policy home

[Sysname-wips-cms-home] countermeasure mac-address 2a11-1fa1-141f

2.1.39 countermeasure misassociation-client

Syntax

countermeasure misassociation-client

undo countermeasure misassociation-client

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure misassociation-client コマンドは間違って関連付けられたクライアントに対策を講じるために WIPS を有効にします。

undo countermeasure misassociation-client コマンドはデフォルトに戻します。

例

間違って関連付けられたクライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure misassociation-client

2.1.40 countermeasure misconfigured-ap

Syntax

countermeasure misconfigured-ap

undo countermeasure misconfigured-ap

デフォルト

設定なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure misconfigured-ap コマンドは誤って設定した AP に対策を講じるために WIPS を有効にします。

undo countermeasure misconfigured-ap コマンドはデフォルトに戻します。

例

誤って設定した AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure misconfigured-ap

2.1.41 countermeasure policy

Syntax

countermeasure policy *policy-name*

undo countermeasure policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザーロール

network-admin

パラメータ

policy-name: 対策ポリシーの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

countermeasure policy コマンドは対策ポリシーを作成し、その view に移行します。

undo countermeasure policy コマンドは対策ポリシーを削除します。

例

対策ポリシーhome を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home]

2.1.42 countermeasure potential-authorized-ap

Syntax

countermeasure potential-authorized-ap

undo countermeasure potential-authorized-ap

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure potential-authorized-ap コマンドは潜在的許可 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-authorized-ap コマンドはデフォルトに戻します。

例

潜在的許可 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure potential-authorized-ap

2.1.43 countermeasure potential-external-ap

Syntax

countermeasure potential-external-ap

undo countermeasure potential-external-ap

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure potential-external-ap コマンドは潜在的外部 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-external-ap コマンドはデフォルトに戻します。

例

潜在的外部 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure potential-external-ap

2.1.44 countermeasure potential-rogue-ap

Syntax

countermeasure potential-rogue-ap

undo countermeasure potential-rogue-ap

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure potential-rogue-ap コマンドは潜在的不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-rogue-ap コマンドはデフォルトに戻します。

例

潜在的不正 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure potential-rogue-ap

2.1.45 countermeasure rogue-ap

Syntax

countermeasure rogue-ap

undo countermeasure rogue-ap

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure rogue-ap コマンドは不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure rogue-ap コマンドはデフォルトに戻します。

例

不正 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure rogue-ap

2.1.46 countermeasure unauthorized-client

Syntax

countermeasure unauthorized-client

undo countermeasure unauthorized-client

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure unauthorized-client コマンドは、未承認のクライアントに対して WIPS を有効にします。

undo countermeasure unauthorized-client コマンドは、デフォルトに戻します。

例

#未承認のクライアントに対して WIPS を有効にします。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] countermeasure policy home

[Sysname-wips-cms-home] countermeasure unauthorized-client

2.1.47 countermeasure uncategorized-ap

Syntax

countermeasure uncategorized-ap

undo countermeasure uncategorized-ap

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure uncategorized-ap コマンドは、未分類の AP に対して WIPS を有効にします。

undo countermeasure uncategorized-ap コマンドは、デフォルトに戻します。

例

未分類 AP に対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure uncategorized-ap

2.1.48 countermeasure uncategorized-client

Syntax

countermeasure uncategorized-client

undo countermeasure uncategorized-client

デフォルト

対策なし

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

countermeasure unauthorized-client コマンドは無許可クライアントに対策を講じるために WIPS を有効にします。

undo countermeasure unauthorized-client コマンドはデフォルトに戻します。

例

無許可クライアントに対策を講じるために WIPS を有効にします。

<AC> system-view

[AC] wips

[AC-wips] countermeasure policy home

[AC-wips-cms-home] countermeasure unauthorized-client

2.1.49 deauthentication-broadcast

Syntax

deauthentication-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo deauthentication-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証解除フレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計情報収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証解除攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。WIPS は遅延時間内にブロードキャスト認証解除攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証解除攻撃アラームを引き起こすブロードキャスト認証解除の数を指定します。threshold-value 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

deauthentication-broadcast コマンドはブロードキャスト認証解除攻撃検出を設定します。

undo deauthentication-broadcast コマンドはブロードキャスト認証解除攻撃検出を無効にします。

例

ブロードキャスト認証解除攻撃検出を有効にします。interval-value、quiet-value、threshold-value の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] deauthentication-broadcast interval 100 threshold 100 quiet 360

2.1.50 detect dissociate-client enable

Syntax

detect dissociate-client enable

undo detect dissociate-client enable

デフォルト

無効

View

Attack detection view

定義済みユーザーロール

network-admin

説明

detect dissociate-client enable コマンドを使用して、WIPS のクライアント検出機能を有効にします。

undo detect dissociate-client enable コマンドを使用して、WIPS 検出のクライアント側の機能を無効にします。

例

#WIPS を有効にして、クライアントを検出します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] detect dissociate-client enable

2.1.51 detect policy

Syntax

detect policy *policy-name*

undo detect policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザーロール

network-admin

パラメータ

policy-name: 攻撃検出ポリシーの名前を指定します。大文字と小文字を区別します。設定範囲は 1～63 文字です。

説明

detect policy コマンドは攻撃検出ポリシーを作成し、その view に移行します。

undo detect policy コマンドは攻撃検出ポリシーを削除します。

例

攻撃検出ポリシーhome を作成し、その view に移行します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home]

2.1.52 detect signature

Syntax

detect signature [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo detect

デフォルト

有効

View

Signature policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: 署名に一致するパケットのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトは 60 秒です。

quiet *quiet-value*: WIPS が user-defined 攻撃アラームをトリガーしてからの遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内に user-defined 攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*:攻撃アラームをトリガーする署名に一致したパケット数を指定します。threshold-value 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

detect signature コマンドは署名に基づく攻撃検出を有効にします。

undo detect signature コマンドは署名に基づく攻撃検出を無効にします。

例

署名に基づく user-define 攻撃検出を有効にします。interval-value、quiet-value、threshold-value の値をそれぞれ、60、100、360 に設定します。

<AC> system-view

[AC] wips

[AC-wips] signature policy home

[AC-wips-sig-home] detect signature interval 60 threshold 100 quiet 360

2.1.53 disassociation-broadcast

Syntax

disassociation-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo disassociation-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証解除フレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計情報収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証解除攻撃アラームをトリガーした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内にブロードキャスト認証解除攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証解除攻撃アラームをトリガーするブロードキャスト認証解除フレーム数を指定します。threshold-value 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

disassociation-broadcast コマンドはブロードキャスト認証解除攻撃検出を有効にします。

undo disassociation-broadcast コマンドはブロードキャスト認証解除攻撃検出を無効にします。

例

ブロードキャスト認証解除攻撃検出を有効にします。interval-value、quiet-value、threshold-value の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] disassociation-broadcast interval 100 threshold 100 quiet 360

2.1.54 discovered-ap

Syntax

discovered-ap *value1* [**to** *value2*]

undo discovered-ap

デフォルト

一致なし

View

AP classification rule view

定義済みユーザーロール

network-admin

パラメータ

value 1 **to** *value 2:*AP を検出するセンサーの数の値の範囲を指定します。*value 1* 引数と *value 2* 引数は、それぞれ値の範囲の開始値と終了値を指定します。値の範囲は、value 1 引数と *value 2* 引数の両方で 1 から 128 であり、*value 2* は *value 1* より大きくなければなりません。

説明

dscovered-ap コマンドは、AP 分類ルールで AP を検出する センサー の数を一致させるために使用されます。

undo discover-ap コマンドは、デフォルトに戻します。

例

#ID 1 の AP 分類ポリシーで、検出された AP の数が 10 を超える AP に一致するようにセンサーを設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] ap-classification rule 1

[Sysname-wips-cls-rule-1] discovered-ap 10 to 128

2.1.55 display wips sensor

Syntax

display wips sensor

View

すべての view

定義済みユーザーロール

network-admin

network-operator

説明

display wips sensor コマンドはすべてのセンサーに関する情報を表示します。

例

すべてのセンサーに関する情報を表示します。

<Sysname> display wips sensor

Total number of sensors: 1

Sensor ID	Sensor name	VSD name	Radio ID	Status
3	ap1	aaa	1	Active

表 2-1 コマンド出力

フィールド	説明
VSD name	アクセスポイントが属するVSD名
Radio ID	WIPSを有効にするRadio ID
Status	センサーの状態 ● active－センサーはWIPSで有効にされます。 ● Inactive－センサーはWIPSで有効にされません。

2.1.56 display wips statistics

Syntax

display wips statistics [**receive** | **virtual-security-domain** *vsd-name*]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

receive: すべての VSD のセンサーから AC が受信する攻撃検出統計情報情報を表示します。

virtual-security-domain vsd-**name**: 指定された VSD のセンサーから AC が受信する攻撃検出統計情報情報を表示します。

説明

display wips statistics コマンドはセンサーから収集した攻撃検出情報を表示します。

例

すべての VSD のセンサーから収集した攻撃検出統計情報を表示します。

<Sysname> display wips statistics receive

Information from sensor 1

Information about attack statistics:

Detected association-request flood messages: 0

Detected authentication flood messages: 0

Detected beacon flood messages: 0

Detected block-ack flood messages: 0

Detected cts flood messages: 0

Detected deauthentication flood messages: 0

Detected disassociation flood messages: 0

Detected eapol-start flood messages: 0

Detected null-data flood messages: 0

Detected probe-request flood messages: 0

Detected reassociation-request flood messages: 0

Detected rts flood messages: 0

Detected eapol-logoff flood messages: 0

Detected eap-failure flood messages: 0

Detected eap-success flood messages: 0

Detected duplicated-ie messages: 0

Detected fata-jack messages: 0

Detected illegal-ibss-ess messages: 0

Detected invalid-address-combination messages: 0

Detected invalid-assoc-req messages: 0

Detected invalid-auth messages: 0

Detected invalid-deauth-code messages: 0

Detected invalid-disassoc-code messages: 0

Detected invalid-ht-ie messages: 0

Detected invalid-ie-length messages: 0

Detected invalid-pkt-length messages: 0

Detected large-duration messages: 0

Detected null-probe-resp messages: 0

Detected overflow-eapol-key messages: 0

Detected overflow-ssid messages: 0

Detected redundant-ie messages: 0

Detected AP spoof AP messages: 0

Detected AP spoof client messages: 0

Detected AP spoof ad-hoc messages: 0

Detected ad-hoc spoof AP messages: 0

Detected client spoof AP messages: 0

Detected weak IV messages: 0

Detected excess AP messages: 0

Detected excess client messages: 0

Detected signature rule messages: 0

Detected 40MHZ messages: 0

Detected power save messages: 0

Detected omerta messages: 0

Detected windows bridge messages: 0

Detected soft AP messages: 0

Detected broadcast disassoc messages: 0

Detected broadcast deauth messages: 0

Detected AP impersonate messages: 0

Detected HT greenfield messages: 0

Detected association table overflow messages: 0

Detected wireless bridge messages: 0

Detected AP flood messages: 0

表 2-2 コマンド出力

フィールド	説明
Information from sensor n	センサーnから収集される情報（nはセンサーのIDを表す）。
Detected association-request flood messages	アソシエーション要求フラッド攻撃で検出されたメッセージの数。
Detected authentication flood messages	認証要求フラッド攻撃に対して検出したメッセージの数。
Detected beacon flood messages	ビーコンフラッド攻撃に対して検出したメッセージの数。
Detected block-ack flood messages	Brock Ackフラッド攻撃に対して検出したメッセージの数。
Detected cts flood messages	CTSフラッド攻撃に対して検出したメッセージの数。
Detected deauthentication flood messages	認証解除フラッド攻撃に対して検出したメッセージの数。
Detected disassociation flood messages	アソシエーション解除フラッド攻撃に対して検出したメッセージの数。
Detected eapol-start flood messages	EAPOLスタートフラッド攻撃に対して検出したメッセージの数。
Detected null-data flood messages	nullデータフラッド攻撃に対して検出したメッセージの数。

フィールド	説明
Detected probe-request flood messages	プローブ要求フラッド攻撃に対して検出したメッセージの数。
Detected reassociation-request flood messages	再関連付け要求フラッド攻撃に対して検出したメッセージの数。
Detected rts flood messages	RTSフラッド攻撃に対して検出したメッセージの数。
Detected eapol-logoff flood messages	EAPOLログオフフラッド攻撃に対して検出したメッセージの数。
Detected eap-failure flood messages	EAPOL失敗フラッド攻撃に対して検出したメッセージの数。
Detected eap-success flood messages	EAPOL成功フラッド攻撃に対して検出したメッセージの数。
Detected duplicated-ie messages	複製されたIEをもつ異常パケットに対して検出したメッセージの数。
Detected fata-jack messages	FATAジャック不正パケットに対して検出したメッセージの数。
Detected illegal-ibss-ess messages	不正なIBSSとESS設定をもつ異常パケットに対して検出したメッセージの数。
Detected invalid-address-combination messages	無効な送信元アドレスをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-assoc-req messages	異常な関連付け要求に対して検出したメッセージの数。
Detected invalid-auth messages	異常な認証要求に対して検出したメッセージの数。
Detected invalid-deauth-code messages	無効な認証解除コードをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-disassoc-code messages	無効な関連付け解除コードをもつ不正パケットに対して検出したメッセージの数。
Detected invalid-ht-ie messages	不正なHT IEをもつ不正パケットに対して検出したメッセージの数。
Detected invalid-ie-length messages	無効なIE長をもつ不正パケットに対して検出したメッセージの数。
Detected invalid-pkt-length messages	無効なパケット長をもつ不正パケットに対して検出したメッセージの数。
Detected large-duration messages	オーバーサイズの期間をもつ不正パケットに対して検出したメッセージの数。
Detected null-probe-resp messages	不正なプローブ要求フレームに対して検出したメッセージの数。
Detected overflow-eapol-key messages	オーバーサイズのEAPOL鍵をもつ不正パケットに対して検出したメッセージの数。
Detected overflow-ssid messages	オーバーサイズなSSIDをもつ不正パケットに対して検出したメッセージの数。

フィールド	説明
Detected redundant-ie messages	冗長なIEをもつ不正パケットに対して検出したメッセージの数。
Detected AP spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs AP)
Detected AP spoof client messages	クライアントスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs client)
Detected AP spoof ad-hoc messages	アドホックスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs Ad hoc)
Detected ad-hoc spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(Ad hoc spoofs AP)
Detected client spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(client spoofs AP)
Detected weak IV messages	ウィークIVに対して検出したメッセージの数。
Detected excess AP messages	APエントリ攻撃に対して検出したメッセージの数。
Detected excess client messages	クライアントエントリ攻撃に対して検出したメッセージの数。
Detected 40MHZ messages	40Hz帯モードで無効化されるクライアントに対して検出したメッセージの数。
Detected power save messages	電力節約攻撃に対して検出したメッセージの数。
Detected omerta messages	Omerta攻撃に対して検出したメッセージの数。
Detected windows bridge messages	Windowsブリッジに対して検出したメッセージの数。
Detected soft AP messages	ソフトAPメッセージが検出されたエスカレーション数
Detected broadcast disassoc messages	ブロードキャスト関連付け解除攻撃に対して検出したメッセージの数。
Detected broadcast deauth messages	ブロードキャスト認証解除フレームメッセージのエスカレーション数が検出されました
Detected AP impersonate messages	ブロードキャスト認証解除攻撃に対して検出したメッセージの数。
Detected HT greenfield messages	HTグリーンフィールドAPの検出メッセージ数
Detected association table overflow messages	アソシエーション/再アソシエーションのDoS攻撃に対する検出メッセージ数
Detected wireless bridge messages	無線ブリッジの検出メッセージ数。
Detected AP flood messages	APフラッドアタックの検出メッセージ数

関連コマンド

- **reset wips statistics**

2.1.57 display wips virtual-security-domain countermeasure record

Syntax

display wips virtual-security-domain *vsd-name* **countermeasure record**

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

display wips virtual-security-domain countermeasure record コマンドは WIPS が不正な装置に実行している対策情報を表示します。

例

VSD office で WIPS が対策を実行している不正な装置に関する情報を表示します。

<Sysname> display wips virtual-security-domain office countermeasure record

Total 3 times countermeasure, current 3 countermeasure record in virtual-security-domain office

Reason: Att - attack; Ass - associated; Black - blacklist;
Class - classification; Manu - manual;

MAC address	Type	Reason	Countermeasure AP	Radio ID	Time
1000-0000-00e3	AP	Manu	ap1	1	2016-05-03/09:32:01
1000-0000-00e4	AP	Manu	ap2	1	2016-05-03/09:32:11
2000-0000-f282	Client	Black	ap3	1	2016-05-03/09:31:56

表 2-3 コマンド出力

フィールド	説明
Total *number* times countermeasure, current *number* countermeasure record in virtual-security-domain *number*	成功した対策の数。このフィールドは最大1024まで表示できます。

フィールド	説明
MAC Address	WIPSが有効になった無線デバイスのMACアドレス
Type	無線デバイスのタイプ: ● AP ● Client
Reason	WIPSが有効にになった理由。 ● Attackー無線デバイスが攻撃者であるため無線デバイスに対して対策します。 ● Assー無線デバイスが関連付いたAPに対して対策します。 ● Blackークライアントに対策後にAPに関連付くと、クライアントをブラックリストに追加します。 ● Classーデバイスのタイプに基づいて対策を実施します。 ● Manuーマックアドレスに基づいて対策を実施します。
Countermeasure AP	無線デバイスに対策を実行したセンサーの名前。
Radio ID	無線デバイスに対策を実行したセンサーの無線ID。
Time	無線デバイスに対策を実行した時間。

関連コマンド

- **reset wips virtual-security-domain countermeasure record**

2.1.58 display wips virtual-security-domain device

Syntax

display wips virtual-security-domain *vsd-name* **device**

[**ap** [**ad-hoc** | **authorized** | **external** | **mesh** | **misconfigured** | **potential-authorized** | **potential-external** | **potential-rogue** | **rogue** | **uncategorized**] | **client** [[**dissociative-client**] | [**authorized** | **misassociation** | **unauthorized** | **uncategorized**]] | **mac-address** *mac-address*] [**verbose**]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 無線デバイスを指定します。

ap: AP を指定します。

ad-hoc: アドホックモードで動作する AP を指定します。

authorized: 許可された AP 指定します。

external: 外部 AP を指定します。

misconfigured: 間違って設定された AP を指定します。

mesh : メッシュリンクを指定します。

potential-authorized: 潜在的に許可された AP を指定します。

potential-external: 潜在的外部 A を指定します。

potential-rogue: 潜在的な不正 AP を指定します。

rogue: 不正な AP を指定します。

client: クライアントを指定します。

dissociative-client: 関連付けられていないクライアントを指定します。

authorized: 許可されたクライアントを指定します。

misassociation: 間違って関連付けられたクライアントを指定します。

unauthorized: 未許可クライアントを指定します。

uncategorized: 分類されていないクライアントを指定します。

mac-address *mac-address*: 無線デバイス MAC アドレスの H-H-H 形式で指定します。

verbose: 詳細なデバイス情報を表示します。

説明

display wips virtual-security-domain device コマンドは VSD で検出された無線装置に関する情報を表示します。

例

VSD office で検出された無線装置に関する情報を表示します。

<Sysname> display wips virtual-security-domain office device

Total 3 detected devices in virtual-security-domain office

Class: Auth - authorization; Ext - external; Mis - mistake;

Unauth - unauthorized; Uncate - uncategorized;

(A) - associate; (C) - config; (P) - potential;

Ad-hoc; Mesh

MAC address	Type	Class	Duration	Sensors	Channel	Status
1000-0000-0000	AP	Ext(P)	00h 10m 46s	1	11	Active
1000-0000-0001	AP	Ext(P)	00h 10m 46s	1	6	Active
1000-0000-0002	AP	Ext(P)	00h 10m 46s	1	1	Active

表 2-4 コマンド出力

フィールド	説明
Type	無線装置タイプ : AP、Client、または Mesh
Class	無線装置のカテゴリ
Duration	無線装置が現在の状態に移行してからの期間
Sensors	無線装置を検出したセンサーの数
Channel	直近で無線装置が検出されたチャネル
Status	APまたはクライアントテーブルエントリのステータス: ● Active:AP またはクライアントがアクティブです ● Inactive:AP またはクライアントが非アクティブです

VSD a で検出された無線装置に関する詳細な情報を表示します。

<Sysname> display wips virtual-security-domain a device verbose

Total 2 detected devices in virtual-security-domain a

AP: 1000-0000-0000

Mesh Neighbor: None

Classification: Mis(C)

Severity level: 0

Classify way: Auto

Status: Active

Status duration: 00h 27m 57s

Vendor: Not found

SSID: service

Radio type: 802.11g

Countermeasuring: No

Security: None

Encryption method: None

Authentication method: None

Broadcast SSID: Yes

QoS supported: No

Ad-hoc: No

Beacon interval: 100 TU

Up duration: 00h 27m 57s

Channel band-width supported: 20MHZ

Hotspot AP: No

Soft AP: No

Honeypot AP: No

Total number of reported sensors: 1

Sensor 1:

Sensor ID: 3

Sensor name: 1

Radio ID: 1

RSSI: 15

Channel: 149

First reported time: 2014-06-03/09:05:51

Last reported time: 2014-06-03/09:05:51

Total number of associated clients: 1

01: 2000-0000-0000

Client: 2000-0000-0000

Last reported associated AP: 1000-0000-0000

Classification: Uncate

Severity level: 0

Classify way: Auto

Dissociative status: No

Status: Active

Status duration: 00h 00m 02s

Vendor: Not found

Radio type: 802.11a

40mhz intolerance: No

Countermeasuring: No

Man in the middle: No

Total number of reported sensors: 1

Sensor 1:

Sensor ID: 2

Sensor name: 1

Radio ID: 1

RSSI: 50

Channel: 149

First reported time: 2014-06-03/14:52:56

Last reported time: 2014-06-03/14:52:56

Reported associated AP: 1000-0000-0000

表 2-5 コマンド出力

フィールド	説明
AP	APのMACアドレス
Mesh Neighbor	Mesh APネイバーのMACアドレス
Client	クライアントのMACアドレス
Last reported associated AP	クライアントが直近で報告した、関連付けられたAPのMACアドレス

フィールド	説明
Classification	APまたはワイヤレスクライアントの分類: ● AP デバイスには次のタイプがあります。 ● ad_hoc:Ad hoc ● authorized ● rogue ● misconfigured ● external ● potential-authorized ● potential-rogue ● potential-external ● uncategorized ● ワイヤレスクライアントには、次のタイプがあります。 ● authorized ● unauthorized ● misassociated ● uncategorized
Severity level	デバイスのセキュリティレベル
Classify way	APまたは無線デバイスの分類方法: ● Manual:手動分類 ● Invalid OUI:無効な OUI リストに追加 ● Block List:禁止装置リストに追加 ● Associated:AC に接続された AP ● Trust List:許可装置リストに追加 ● User Define:ユーザーが定義した分類 ● Auto Auto Auto:自動分類
Dissociative status	クライアントが関連付けられていないクライアントかどうか。
Status	APまたはクライアントテーブルエントリのステータス: ● Active:AP またはクライアントがアクティブです ● Inactive:AP またはクライアントが非アクティブです
Status duration	デバイスの現在の状態の継続時間

フィールド	説明
Vendor	装置のOUI。装置のOUIが、インポートされたOUIと一致する場合、このフィールドは装置のOUIを表示します。装置にOUIが設定されていない場合、あるいは装置のOUIが、インポートされたいずれのOUIとも一致しない場合、このフィールドはNot foundと表示されます。
SSID	APが提供するSSID
Radio Type	無線デバイスの無線モード
40 MHz intolerance	クライアントが40MHz帯をサポートするかどうかをあらわします。
Countermeasuring	WIPSが無線デバイスに対して対策を講じているかどうか: ● No ● Yes
Man in the middle	MITM攻撃を検出するかどうかをあらわします。
Security	セキュリティ方式: ● None ● WEP ● WPA ● WPA 2 ● WAPI
Encryption method	データの暗号化方式: ● TKIP ● CCMP ● WEP ● WAPI ● None
Authentication method	認証方式: ● None ● PSK ● 802.1 X ● Others
Broadcast SSID	APがSSIDをブロードキャストするかどうかをあらわします。APがSSIDをブロードキャストしない場合、このフィールドは何も表示しません。
QoS supported	無線デバイスがQoSをサポートするかどうかをあらわします。
Ad-hoc	無線デバイスがアドホックモードかどうかをあらわします。

フィールド	説明
Beacon interval	TUにおけるビーコン間隔です。1つのTUは1024マイクロ秒に等しいです。
Up duration	APデバイスの起動から現在までの時間
Channel band-width supported	サポートされるチャネル帯域幅: ● 20/40/80 MHZ ● 20/40 MHZ
Hotspot AP	APがホットスポット攻撃APであるかどうかをあらわします。
Soft AP	APがソフトAPであるかどうかをあらわします。
Honeypot AP	APがハニーポットAPであるかどうかをあらわします。
センサー n	無線デバイスを検出したセンサーです。n はシステムに割り当てられたIDをあらわします。
センサー ID	センサーのAPID
センサー name	センサー名
Radio ID	センサーのRadio ID
RSSI	センサーの信号強度
Channel	センサーが検出した装置のチャネル
First reported time	センサーがAPまたは無線デバイスを最初に検出した時刻
Last reported time	このセンサーがAPまたは無線デバイスを最後に検出した時刻
Total number of associated clients	デバイスに関連付けられているClientの数
n:H-H-H	APに関連付けられている無線デバイスのMACアドレス。nはシステム自動番号。
Reported associated AP	センサーが報告した、関連付けられたAPのMACアドレスです。

関連コマンド

- **reset wips virtual-security-domain device**

2.1.59 display wlan nat-detect

Syntax

display wlan nat-detect [**mac-address** *mac-address*]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントを MAC アドレスで指定します。このオプションを指定しない場合、検出されたすべての NAT 構成クライアントに関する情報が表示されます。

説明

display wlan nat-detect コマンドは NAT が設定されたクライアントに関する情報を表示します。

例

検出されたすべての NAT 構成クライアントに関する情報を表示します。

<Sysname> display wlan nat-detect

Total 1 detected clients with NAT configured

MAC address Last report First report Duration

0a98-2044-0000 2017-08-24/11:05:23 2017-08-24/10:05:23 01h 15m 00s

表 2-6 コマンド出力

フィールド	説明
Total number detected clients with NAT configured	検出されたNAT構成クライアントの数
MAC address	検出されたクライアントのMACアドレス
Last report	クライアントが直近に検出された時刻
First report	クライアントが最初に検出された時刻
Duration	クライアントがNAT設定されてからの期間

関連コマンド

- **reset wlan nat-detect**

2.1.60 flood association-request

Syntax

flood association-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood association-request

デフォルト

無効

View

Attack detection view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: 関連付け要求フレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が関連付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に関連付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 関連付け要求フラッド攻撃アラームを引き起こす関連付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood association-request コマンドは関連付け要求フラッド攻撃検出を設定します。

undo flood association-request コマンドはデフォルトに戻します。

例

関連付け要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood association-request interval 100 threshold 100 quiet 360

2.1.61 flood authentication

Syntax

flood authentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood authentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network admin

パラメータ

interval *interval-value*: 認証要求フレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証要求フラッド攻撃アラームを引き起こす認証要求フレーム数を指定します。threshold-value 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood authentication コマンドは認証要求フラッド攻撃検出を設定します。

undo flood authentication コマンドはデフォルトに戻します。

例

認証要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood authentication interval 100 threshold 100 quiet 360

2.1.62 flood beacon

Syntax

flood beacon [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood beacon

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: ビーコンフレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がビーコンフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にビーコンフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ビーコンフラッド攻撃アラームを引き起こすビーコンフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood beacon コマンドはビーコンフラッド攻撃検出を設定します。

undo flood beacon コマンドはデフォルトに戻します。

例

ビーコンフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood beacon interval 100 threshold 100 quiet 360

2.1.63 flood block-ack

Syntax

flood block-ack [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood block-ack

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: ブロックアックフレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロックアックフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にブロックアックフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロックアックフラッド攻撃アラームを引き起こすブロックアックフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood block-ack コマンドはブロックアックフラッド攻撃検出を設定します。

undo flood block-ack コマンドはデフォルトに戻します。

例

ブロックアックフラッド攻撃検出を有効にします。interval-value、quiet-value、threshold-value の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood block-ack interval 100 threshold 100 quiet 360

2.1.64 flood cts

Syntax

flood cts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood cts

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: CTS フレームの統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が CTS フラッド攻撃アラームを引き起こしてからの遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に CTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: CTS フラッド攻撃アラームを引き起こす CTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood cts コマンドは CTS フラッド攻撃検出を設定します。

undo flood cts コマンドはデフォルトに戻します。

例

CTS フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood cts interval 100 threshold 100 quiet 360

2.1.65 flood deauthentication

Syntax

flood deauthentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood deauthentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: 認証解除フレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証解除フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証解除フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証解除フラッド攻撃アラームを引き起こす認証解除フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood deauthentication コマンドは認証解除フラッド攻撃検出を設定します。

undo flood deauthentication コマンドはデフォルトに戻します。

例

認証解除フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood deauthentication interval 100 threshold 100 quiet 360

2.1.66 flood disassociation

Syntax

flood disassociation [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood disassociation

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: 関連付け解除フレームの統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が関連付け解除フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に関連付け解除フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 関連付け解除フラッド攻撃アラームを引き起こす関連付け解除フレーム数を指定します。threshold-value 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood disassociation コマンドは関連付け解除フラッド攻撃検出を設定します。

undo flood disassociation コマンドはデフォルトに戻します。

例

関連付け解除フラッド攻撃検出を有効にします。interval-value、quiet-value、threshold-value の値をそれぞれ、100、100、360 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood disassociation interval 100 threshold 100 quiet 360

2.1.67 flood eap-failure

Syntax

flood eap-failure [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-failure

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: EAP 失敗フレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAP 失敗フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAP 失敗フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAP 失敗フラッド攻撃アラームを引き起こす EAP 失敗フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eap-failure コマンドは EAP 失敗フラッド攻撃検出を設定します。

undo flood eap-failure コマンドはデフォルトに戻します。

例

EAP 失敗フラッド攻撃検出を有効にします。interval-value、quiet-value、threshold-value の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood eap-failure interval 100 threshold 100 quiet 360

2.1.68 flood eapol-logoff

Syntax

flood eapol-logoff [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-logoff

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: EAPOL ログオフフレームの統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL ログオフフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL ログオフフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL ログオフフラッド攻撃アラームを引き起こす EAPOL ログオフフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-logoff コマンドは EAPOL ログオフフラッド攻撃検出を設定します。

undo flood eapol-logoff コマンドはデフォルトに戻します。

例

EAPOL ログオフフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood eapol-logoff interval 100 threshold 100 quiet 360

2.1.69 flood eapol-start

Syntax

flood eapol-start [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-start

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: EAPOL スタートフレームの統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL スタートフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL スタートフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL スタートフラッド攻撃アラームを引き起こす EAPOL スタートフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-start コマンドは EAPOL スタートフラッド攻撃検出を設定します。

undo flood eapol-start コマンドはデフォルトに戻します。

例

EAPOL スタートフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AC> system-view

[AC] wips

[AC-wips] detect policy home

[AC-wips-dtc-home] flood eapol-start interval 100 threshold 100 quiet 360

2.1.70 flood eap-success

Syntax

flood eap-success [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-success

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*:EAS-success フレームの統計情報収集間隔を指定します。interval-value 引数の値の範囲は 1~3600 秒で、デフォルトの統計情報収集間隔は 60 秒です。

quiet *quiet-value*:EAP-success フラッド攻撃時に WIPS がアラームをトリガーしてからの待機時間を指定します。quiet-value 引数の値の範囲は 5~604800 秒で、デフォルトの待機時間は 600 秒です。WIPS は、待機時間内に EAP 成功フラッド攻撃を検出してもアラームをトリガーしません。

threshold *threshold-value*:EAP-success flood attack アラームをトリガーする EAP-success フレームの数を指定します。threshold-value 引数の値の範囲は 1 から 10 万で、デフォルト値は 50 です。

説明

flood eap-success コマンドは、EAP-Success フレームフラッド攻撃検出機能を有効にするために使用します。

undo flood eap-success コマンドは、EAP-Success フレームフラッド攻撃検出機能を無効にするために使用します。

例

EAP-Success フレームのフラッド攻撃検出機能を有効にします。統計期間は 100 秒、アラームしきい値は 100 秒、 無音時間は 360 秒です。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood eap-success interval 100 threshold 100 quiet 360

2.1.71 flood null-data

Syntax

flood null-data [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood null-data

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: null データフレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が null データフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に null データフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: null データフラッド攻撃アラームを引き起こす null データフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood null-data コマンドは null データフラッド攻撃検出を設定します。

undo flood null-data コマンドはデフォルトに戻します。

例

null データフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood null-data interval 100 threshold 100 quiet 360

2.1.72 flood probe-request

Syntax

flood probe-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood probe-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: プローブ要求フレームの統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がプローブ要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にプローブ要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: プローブ要求フラッド攻撃アラームを引き起こすプローブ要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood probe-request コマンドはプローブ要求フラッド攻撃検出を設定します。

undo flood probe-request コマンドはデフォルトに戻します。

例

プローブ要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood probe-request interval 100 threshold 100 quiet 360

2.1.73 flood reassociation-request

Syntax

flood reassociation-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood reassociation-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: 再関連付け要求フレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が再関連付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に再関連付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 再関連付け要求フラッド攻撃アラームを引き起こす再関連付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood reassociation-request コマンドは再関連付け要求フラッド攻撃検出を設定します。

undo flood reassociation-request コマンドはデフォルトに戻します。

例

再関連付け要求フラッド攻撃検出を有効にします。interval-value、quiet-value、threshold-value の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood reassociation-request interval 100 threshold 100 quiet 360

2.1.74 flood rts

Syntax

flood rts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood rts

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*: RTS フレームのための統計情報収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が RTS フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に RTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: RTS フラッド攻撃アラームを引き起こす RTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood rts コマンドは RTS フラッド攻撃検出を設定します。

undo flood rts コマンドはデフォルトに戻します。

例

#RTS フラッド攻撃検出を有効にします。**interval-value**、**quiet-value**、**threshold-value** の値をそれぞれ、100、360、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] flood rts interval 100 threshold 100 quiet 360

2.1.75 frame-type

Syntax

frame-type { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }

undo frame-type

デフォルト

設定なし

View

Sgnature rule view

定義済みユーザーロール

network-admin

パラメータ

control: 制御フレームと整合します。

data: データフレームと整合します。

management: 管理フレームと整合します。

frame-subtype: フレームサブタイプを指定します。

association-request: 関連付け要求フレームと整合します。

association-response: 関連付け応答フレームと整合します。

authentication: 認証フレームと整合します。

beacon: ビーコンフレームと整合します。

deauthentication: 認証解除フレームと整合します。

disassociation: 関連付け解除フレームと整合します。

probe-request: プローブ要求フレームと整合します。

説明

frame-type コマンドはフレームのフレームタイプと整合するためにサブ署名を設定します。

undo frame-type コマンドはデフォルトに戻します。

例

データフレームと一致するように signature 1 に対してサブ署名を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature rule 1

[wips-sig-rule-1] frame-type data

関連コマンド

- **mac-address**
- **seq-number**
- **ssid-length**
- **ssid (signature rule view)**
- **pattern**
- **match all (signature rule view)**

2.1.76 honeypot-ap

Syntax

honeypot-ap [**similarity** *similarity-value* | **quiet** *quiet-value*] *

undo honeypot-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

similarity *similarity-value*: ハニーポット AP アラームを引き起こす類似のしきい値を指定します。値の範囲は 70～100%です。デフォルト値は 80%です。AP の SSID と適合 AP の SSID との間の類似点がしきい値に達すると、AP はハニーポット AP とみなされます。

quiet *quiet-value*: WIPS がハニーポット AP 検出アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット AP を検出してもアラームを引き起こしません。

説明

honeypot-ap コマンドはハニーポット AP 検出を設定します。

undo honeypot-ap コマンドはハニーポット AP 検出を無効にします。

例

ハニーポット AP 検出を有効にします。類似のしきい値と遅延時間をそれぞれ、90%、10 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] honeypot-ap similarity 90 quiet 10

2.1.77 hotspot-attack

Syntax

hotspot-attack [**quiet** *quiet-value*]

undo hotspot-attack

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がハニーポット攻撃アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット攻撃を検出してもアラームを引き起こしません。

説明

hotspot-attack コマンドはハニーポット攻撃検出を設定します。

undo hotspot-attack コマンドはハニーポット攻撃検出を無効にします。

例

ハニーポット攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] hotspot-attack quiet 100

関連コマンド

- **import hotspot**

2.1.78 ht-40mhz-intolerance

Syntax

ht-40mhz-intolerance [**quiet** *quiet-value*]

undo ht-40mhz-intolerance

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が 40MHz の帯域幅モードを使用禁止にしたクライアントを検出するアラームを開始した後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を設定します。

undo ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を無効にします。

例

40MHz の帯域幅モードを使用禁止にしたクライアント検出を有効にします。遅延時間を 100 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] ht-40mhz-intolerance quiet 100

2.1.79 ht-greenfield

Syntax

ht-greenfield [**quiet** *quiet-value*]

undo ht-greenfield

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が HT グリーンフィールド AP 検出アラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-greenfield コマンドは HT グリーンフィールド検出を設定します。

undo ht-greenfield コマンドは HT グリーンフィールド検出を無効にします。

例

HT グリーンフィールド AP 検出を有効にします。遅延時間を 100 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] ht-greenfield quiet 100

2.1.80 ignorelist

Syntax

ignorelist mac-address *mac-address*

undo ignorelist mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザーロール

network-admin

パラメータ

mac-address: MAC アドレスを H-H-H 形式で指定します。

all: アラームを無視する装置リスト内のすべてのすべての MAC アドレスを指定します。

説明

ignorelist コマンドはアラームを無視する装置リストに MAC アドレスを追加します。

undo ignorelist コマンドはアラームを無視する装置リストから特定の、もしくはすべての MAC アドレスを削除します。

例

アラームを無視する装置リストに MAC アドレス 2a11-1fa1-1311 を追加します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] ignorelist mac-address 2a11-1fa1-1311

2.1.81 import hotspot

Syntax

import hotspot *file-name*

undo import hotspot

デフォルト

設定なし

View

WIPS view

定義済みユーザーロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import hotspot コマンドはコンフィグレーションファイルからホットスポットをインポートします。

undo import hotspot コマンドはコンフィグレーションファイルを削除します。

1 つのコンフィグレーションファイルからのみホットスポットをインポートできます。

例

コンフィグレーションファイル hotspot_cfg からホットスポットをインポートします。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] import hotspot hotspot_cfg

関連コマンド

- **hotspot-attack**

2.1.82 import oui

Syntax

import oui *file-name*

undo import oui

デフォルト

インポートなし

View

WIPS view

定義済みユーザーロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import oui コマンドはコンフィグレーションファイルから OUI をインポートします。

undo import oui コマンドはコンフィグレーションを削除します。

IEEE ウェブサイトからコンフィグレーションファイルをダウンロードできます。

1 つのコンフィグレーションファイルからのみ OUI をインポートできます。

例

コンフィグレーションファイル oui_import_cfg から OUI をインポートします。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] import oui oui_import_cfg

関連コマンド

- **export oui**
- **reset wips embedded-ou**

2.1.83 invalid-oui-classify illegal

Syntax

invalid-oui-classify illegal

undo invalid-oui-classify

デフォルト

無効

View

Classification policy view

定義済みユーザーロール

network-admin

説明

invalid-oui-classify illegal コマンドは無効な OUI で装置を不正な装置として分類するように WIPS を有効にします

undo invalid-oui-classify コマンドはデフォルトに戻します。

例

無効な OUI で装置を不正な装置として分類するように WIPS を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] classification policy home

[Sysname-wips-cls-home] invalid-oui-classify illegal

関連コマンド

- **import oui**

2.1.84 mac-address

Syntax

mac-address { **bssid** | **destination** | **source** } *mac-address*

undo mac-address

デフォルト

設定なし

View

Signature

定義済みユーザーロール

network-admin

パラメータ

bssid: 指定された BSSID と整合します。

destination: 指定された送信元 MAC アドレスと整合します。

source: 指定された送信元 MAC アドレスと整合します。

mac-address: MAC アドレスを H-H-H 形式で指定します。

説明

mac-address コマンドはフレームが送信元 MAC アドレスと整合するようにサブ署名を設定します。

undo mac-address コマンドはデフォルトに戻します。

例

フレームが送信元 MAC アドレス 000f-e201-0101 と整合するように signature 1 に対してサブ署名を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature rule 1

[Sysname-wips-sig-rule-1] mac-address source 000f-e201-0101

関連コマンド

- **frame-type**
- **seq-number**
- **ssid-length**
- **ssid (signature rule view)**
- **pattern**
- **match all (signature rule view)**

2.1.85 malformed duplicated-ie

Syntax

malformed duplicated-ie [**quiet** *quiet-value*]

undo malformed duplicated-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が複製された IE のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に複製された IE を検出してもアラームを引き起こしません。

説明

malformed duplicated-ie コマンドは複製された IE を伴った不正パケットを検出するように、WIPS を有効にします。

undo malformed duplicated-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。複製された IE をパケットが持つ場合、WIPS はパケットを不正とみなします。この検出はベンダに定義された IE には適用できません。

例

複製された IE を伴った不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed duplicated-ie quiet 360

2.1.86 malformed fata-jack

Syntax

malformed fata-jack [**quiet** *quiet-value*]

undo malformed fata-jack

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet quiet-value: WIPS が FATA ジャック不正パケットアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に FATA ジャック不正パケットを検出してもアラームを引き起こしません。

説明

malformed fata-jack コマンドは FATA ジャック不正パケットを検出するように、WIPS を有効にします。

undo malformed fata-jack コマンドはデフォルトに戻します。

この機能は認証フレームに適用できます。認証アルゴリズム番号の値が 2 である場合、WIPS は認証フレームを不正とみなします。

例

複製された IE を伴った不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed fata-jack quiet 360

2.1.87 malformed illegal-ibss-ess

Syntax

malformed illegal-ibss-ess [**quiet** *quiet-value*]

undo malformed illegal-ibss-ess

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が不正 IBSS および ESS 設定のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に不正 IBSS および ESS 設定を検出してもアラームを引き起こしません。

説明

malformed illegal-ibss-ess コマンドは不正 IBSS および ESS 設定をもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed illegal-ibss-ess コマンドはデフォルトに戻します。

この機能はビーコンフレームおよびプローブ応答フレームに適用できます。IBSS と ESS がフレーム内でともに 1 に設定されている場合、WIPS はフレームを不正とみなします。

例

不正 IBSS および ESS 設定をもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed illegal-ibss-ess quiet 360

2.1.88 malformed invalid-address-combination

Syntax

malformed invalid-address-combination [**quiet** *quiet-value*]

undo malformed invalid-address-combination

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な送信元アドレスのアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な送信元アドレスを検出してもアラームを引き起こしません。

説明

malformed invalid-address-combination コマンドは無効な送信元アドレスをもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed invalid-address-combination コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。WIPS は以下の条件において、フレームを不正とみなします。

- フレームの TO DS が 1 の場合。（フレームがクライアントにより AP に送信されたことを示します）

- フレームの送信元 MAC アドレスがマルチキャストアドレスもしくはブロードキャストアドレスの場合。

例

無効な送信元アドレスをもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed invalid-address-combination quiet 360

2.1.89 malformed invalid-assoc-req

Syntax

malformed invalid-assoc-req [**quiet** *quiet-value*]

undo malformed invalid-assoc-req

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が不正関連付け要求フレームのアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に不正関連付け要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-assoc-req コマンドは不正関連付け要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-assoc-req コマンドはデフォルトに戻します。

この機能は関連付け要求フレームに適用できます。フレーム内の SSID 長が 0 である場合、WIPS はフレームを不正とみなします。

例

不正関連付け要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed invalid-assoc-req quiet 360

2.1.90 malformed invalid-auth

Syntax

malformed invalid-auth [**quiet** *quiet-value*]

undo malformed invalid-auth

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が不正認証要求フレームのアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に不正認証要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-auth コマンドは不正認証要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-auth コマンドはデフォルトに戻します。

この機能は認証要求フレームに適用できます。WIPS は以下の条件において、フレームを不正とみなします。

- 認証アルゴリズム番号が 802.11 プロトコルと一致せず、3 より大きい場合。
- 認証トランザクションシーケンス番号が 1 であり、状態コードが 0 で無い場合。（認証トランザクションシーケンス番号は、クライアントと AP 間の認証処理を示します。）
- 認証トランザクションシーケンス番号が 4 より大きい場合。

例

不正認証要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed invalid-auth quiet 360

2.1.91 malformed invalid-deauth-code

Syntax

malformed invalid-deauth-code [**quiet** *quiet-value*]

undo malformed invalid-deauth-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な認証解除コードのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な認証解除コードを検出してもアラームを引き起こしません。

説明

malformed invalid-deauth-code コマンドは無効な認証解除コードをもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed invalid-deauth-code コマンドはデフォルトに戻します。

この機能は認証解除フレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを不正とみなします。

例

無効な認証解除コードをもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed invalid-deauth-code quiet 360

2.1.92 malformed invalid-disassoc-code

Syntax

malformed invalid-disassoc-code [**quiet** *quiet-value*]

undo malformed invalid-disassoc-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な関連付け解除コードのアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な関連付け解除コードを検出してもアラームを引き起こしません。

説明

malformed invalid-disassoc-code コマンドは無効な関連付け解除コードをもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed invalid-disassoc-code コマンドはデフォルトに戻します。

この機能は関連付け解除フレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを不正とみなします。

例

無効な関連付け解除コードをもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed invalid-disassoc-code quiet 360

2.1.93 malformed invalid-ht-ie

Syntax

malformed invalid-ht-ie [**quiet** *quiet-value*]

undo malformed invalid-ht-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が不正 HT IE のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に不正 HT IE を検出してもアラームを引き起こしません。

説明

malformed invalid-ht-ie コマンドは不正 HT IE をもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ht-ie コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ応答フレーム、関連付け応答フレーム、再関連付け応答フレームに適用できます。WIPS は以下の条件において、フレームを不正とみなします。

- HT ケーパビリティ IE の SM 電力節約値が 2 である場合。
- HT オペレーション IE のセカンダリチャネルオフセット値が 2 である場合。

例

不正 HT IE をもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed invalid-ht-ie quiet 360

2.1.94 malformed invalid-ie-length

Syntax

malformed invalid-ie-length [**quiet** *quiet-value*]

undo malformed invalid-ie-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な IE 長のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な IE 長を検出してもアラームを引き起こしません。

説明

malformed invalid-ie-length コマンドは無効な IE 長をもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ie-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE 長が 802.11 プロトコルと一致しない場合、WIPS はフレームを不正とみなします。

例

無効な IE 長をもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed invalid-ie-length quiet 360

2.1.95 malformed invalid-pkt-length

Syntax

malformed invalid-pkt-length [**quiet** *quiet-value*]

undo malformed invalid-pkt-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効なパケット長のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効なパケット長を検出してもアラームを引き起こしません。

説明

malformed invalid-pkt-length コマンドは無効なパケット長をもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed invalid-pkt-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。パケットペイロード解析後に IE の残存長が 0 で無い場合、WIPS はフレームを不正とみなします。

例

無効なパケット長をもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed invalid-pkt-length quiet 360

2.1.96 malformed large-duration

Syntax

malformed large-duration [**quiet** *quiet-value* | **threshold** *value*]

undo malformed large-duration

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな期間のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな期間を検出してもアラームを引き起こしません。

threshold *threshold-value*: WIPS がオーバーサイズな期間を判断し、アラームをあげるために、期間のサイズを指定します。value 引数の値の範囲は 1～32767 です。デフォルト値は 5000 です。

説明

malformed large-duration コマンドはオーバーサイズな期間をもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed large-duration コマンドはデフォルトに戻します。

この機能はユニキャスト管理フレーム、ユニキャストデータフレーム、RTS フレーム、CTS フレーム、ACK フレームに適用できます。フレーム内の期間の値が指定されたしきい値より大きい場合、WIPS はフレームを不正とみなします。

例

オーバーサイズな期間をもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed large-duration quiet 360

2.1.97 malformed null-probe-resp

Syntax

malformed null-probe-resp [**quiet** *quiet-value*]

undo malformed null-probe-resp

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が不正プローブ応答フレームのアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に不正プローブ応答フレームを検出してもアラームを引き起こしません。

説明

malformed null-probe-resp コマンドは不正プローブ応答フレームを検出するように、WIPS を有効にします。

undo malformed null-probe-resp コマンドはデフォルトに戻します。

この機能はプローブ応答フレームに適用できます。フレームがメッシュフレームでなく、SSID 長が 0 である場合、WIPS はフレームを不正とみなし、パケットは不正パケットとみなします。

例

不正プローブ応答フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed null-probe-resp quiet 360

2.1.98 malformed overflow-eapol-key

Syntax

malformed overflow-eapol-key [**quiet** *quiet-value*]

undo malformed overflow-eapol-key

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな EAPOL 鍵のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな EAPOL 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-eapol-key コマンドはオーバーサイズな EAPOL 鍵をもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed overflow-eapol-key コマンドはデフォルトに戻します。

この機能は EAPOL キーフレームに適用できます。フレーム内の TO DS が 1 で、鍵長が 0 より大きい場合、WIPS はフレームを不正とみなします。悪意ある EAPOL 鍵フレームにより DOS 攻撃を受ける恐れがあります。

例

オーバーサイズ EAPOL キーをもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed overflow-eapol-key quiet 360

2.1.99 malformed overflow-ssid

Syntax

malformed overflow-ssid [**quiet** *quiet-value*]

undo malformed overflow-ssid

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな SSID のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒

です。WIPS は遅延時間内にオーバーサイズな SSID 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-ssid コマンドはオーバーサイズな SSID をもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed overflow-ssid コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ要求フレーム、プローブ応答フレーム、関連付け要求フレームに適用できます。フレーム内の SSID 長が 32 より大きく、802.11 プロトコルに一致していない場合、WIPS はフレームを不正とみなします。

例

オーバーサイズな SSID をもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed overflow-ssid quiet 360

2.1.100 malformed redundant-ie

Syntax

malformed redundant-ie [**quiet** *quiet-value*]

undo malformed redundant-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value:* WIPS が冗長な IE のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に冗長な IE を検出してもアラームを引き起こしません。

説明

malformed redundant-ie コマンドは冗長な IE をもつ不正パケットを検出するように、WIPS を有効にします。

undo malformed redundant-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE がフレームにとって必要な IE でも予備の IE でもない場合、WIPS はフレームを不正とみなします。

例

冗長な IE をもつ不正パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] malformed redundant-ie quiet 360

2.1.101 man-in-the-middle

Syntax

man-in-the-middle [**quiet** *quiet-value*]

undo man-in-the-middle

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が MITM（Man-In-The-Middle）攻撃のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に MITM 攻撃を検出してもアラームを引き起こしません。

説明

man-in-the-middle コマンドは MITM 攻撃検出を有効にします。

undo man-in-the-middle コマンドは MITM 攻撃検出を無効にします。

MITM 攻撃検出を有効にする前にハニーポット AP 検出を有効にしてください。

例

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] honeypot-ap

[Sysname-wips-dtc-home] man-in-the-middle

2.1.102 manual-classify mac-address

Syntax

manual-classify mac-address *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }

undo manual-classify mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザーロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを H-H-H 形式で指定します。

authorized-ap: AP を許可された AP として指定します。

external-ap: AP を外部 AP として指定します。

misconfigured-ap: AP を間違って設定された AP として指定します。

rogue-ap: AP を不正な AP として指定します。

all: すべての AP を指定します。

説明

manual-classify mac-address コマンドは AP に対してカテゴリを設定します。

undo manual-classify mac-address コマンドはデフォルトに戻します。

例

MAC アドレスが 000f-00e2-0001 の AP を許可された AP として設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] classification policy home

[Sysname-wips-cls-home] manual-classify mac-address 000f-00e2-0001 authorized-ap

2.1.103 match all (AP classification rule view)

Syntax

match all

undo match all

デフォルト

一致

View

AP classification policy view

定義済みユーザーロール

network-admin

説明

match all コマンドを使用して、AP 分類ルールの一致関係を AND に設定します。

undo match all コマンドはデフォルトに戻します。

例

AP 分類ルールの一致関係を AND に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] ap-classification rule 1

[Sysname-wips-cls-rule-1] match all

2.1.104 match all (signature view)

Syntax

match all

undo match all

デフォルト

一致

View

Signature view

定義済みユーザーロール

network-admin

説明

match all コマンドは、Signature ルールの一致関係を AND に設定します。

undo match all コマンドはデフォルトに戻します。

例

#Signature ルール 1 のサブルールの一致関係は AND に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature rule 1

[wips-sig-rule-1] match all

関連コマンド

- **frame-type**
- **mac-address**
- **seq-number**
- **ssid-length**
- **ssid (signature rule view)**
- **pattern**

2.1.105 omerta

Syntax

omerta [**quiet** *quiet-value*]

undo omerta

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Omerta 攻撃のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に Omerta 攻撃を検出してもアラームを引き起こしません。

説明

omerta コマンドは Omerta 攻撃検出を有効にします。

undo omerta コマンドは Omerta 攻撃検出を無効にします。

例

Omerta 攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] omerta quiet 100

2.1.106 oui

Syntax

oui *oui-info*

undo oui

デフォルト

設定なし

View

AP classification rule view

定義済みユーザーロール

network-admin

パラメータ

oui-info: OUI 情報を XXXXXX 形式で指定します。大文字と小文字を区別しません。16 進数で指定します。

説明

oui コマンドは AP の OUI 情報と整合するように AP 分類ルールを設定します。

undo oui コマンドはデフォルトに戻します。

例

AP を OUI 000fe4 と整合するために AP classification rule 1 を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] ap-classification rule 1

[Sysname-wips-cls-rule-1] oui 000fe4

2.1.107 pattern

Syntax

pattern *pattern-number* **offset** *offset-value* **mask** *mask value1* [**to** *value2*] [**from-payload**]

undo pattern { *pattern-number* | **all** }

デフォルト

設定なし

View

Signature view

定義済みユーザーロール

network-admin

パラメータ

pattern-number: フレームの指定ビットに一致するサブシグネチャの番号を 0 から 7 の範囲で指定します。

offset *offset-value*: 指定されたビットから参照ビットまでのオフセットを指定します。offset-value 引数の値の範囲は 0～2346 ビットです。参照ビットは、フレームヘッド（デフォルト）もしくはフレームペイロードの最初のビットになることができます。

mask *mask*: 指定されたビットで AND 演算に使用される 2 バイトマスクを指定します。マスクは 16 進数形式です。マスクの値の範囲は 0～ffff です。

value1 [*to value2*]: ビット数の範囲を指定します。value1 引数と value2 引数は、それぞれ値の範囲の始めと終わりを指定します。value1 引数と value2 引数の値の範囲は、どちらも 0～65535 です。ただし、value2 引数の値は value1 引数の値より大きくなければなりません。

from-payload: 参照ビットとしてフレームペイロードの最初のビットを指定します。このキーワードを指定しない場合、フレームヘッドの最初のビットは参照ビットになります。

説明

pattern コマンドは指定されたフレームのビットと整合するようにサブ署名を設定します。

undo pattern コマンドはデフォルトに戻します。

例

フレームヘッドの第 2 ビットと第 3 ビットが整合するようにサブ署名を設定します。フレームの第 2 ビットと第 3 ビットの値が 0x0015～0x0020 の範囲内の場合、フレームはサブ署名と整合します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature rule 1

[Sysname-wips-sig-rule-1] pattern 1 offset 8 mask ffff 15 to 20

関連コマンド

- **frame-type**
- **mac-address**
- **seq-number**
- **ssid-length**
- **ssid (signature rule view)**
- **match all (signature rule view)**

2.1.108 permit-channel

Syntax

permit-channel *channel-id-list*

undo permit-channel { *channel-id-list* | **all** }

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

channel-id-list: 許可された 10 個までのチャネルアイテムの空間分離リストを指定します。各アイテムは、value1 to value2 の形式でチャネル番号もしくはチャネル番号の範囲を指定します。チャネル番号の範囲は 1～224 です。value2 引数の値は value1 引数の値以上でなければなりません。

all: 許可されたすべてのチャネルを指定します。

説明

permit-channel コマンドは許可されたチャネルリストに 1 つあるいは複数のチャネルを追加します。

undo permit-channel コマンドは許可されたチャネルリストから指定されたチャネルあるいはすべてのチャネルを削除します。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、このコマンドを使用して許可されたチャネルリストを設定します。

例

チャネル 1 を許可されたチャネルリストに追加します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] permit-channel 1

関連コマンド

- **prohibited-channel**

2.1.109 power-save

Syntax

power-save [**interval** *interval-value* | **minoffpacket** *packet-value* | **onoffpercent** *percent-value* | **quiet** *quiet-value*] *

undo power-save

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval *interval-value*:パワーセーブフレームの統計情報収集間隔を指定します。interval-value 引数の値の範囲は 1~3600 秒で、デフォルト値は 10 秒です。

minoffpacket *packet-value*:省電力攻撃分析をトリガーする省電力フレームの数のしきい値を指定します。クライアントからのオフフレームの数がしきい値に達すると、WIPS

は省電力フレームを分析して、省電力攻撃が発生するかどうかを判断します。引数の値の範囲は 10 から 150 で、デフォルトは 50 です。

onoffpercent *percent-value*:クライアントからのフレームのパワーセーブオンとオフフレームの比率のしきい値を指定します。しきい値に達すると、WIPS は省電力攻撃のアラームをトリガーします。この引数の値の範囲は 0 から 100 で、デフォルトは 80 です。

quiet *quiet-value*:省電力攻撃時に WIPS がアラームをトリガーしてからの待機時間を指定します。quiet-value 引数の値の範囲は 5~604800 秒で、デフォルトの待機時間は 600 秒です。WIPS は、待機時間内に省電力攻撃を検出してもアラームをトリガーしません。

説明

power-save コマンドはパワーセーブ攻撃検出を有効にします。

undo power-save コマンドはパワーセーブ攻撃検出を無効にします。

例

パワーセーブ攻撃検出を有効にします。*interval-value*、*packet-value*、*percent-value*、*quiet-value* の値をそれぞれ、20、20、90、100 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] power-save interval 20 minoffpacket 20 onoffpercent 90 quiet 100

2.1.110 prohibited-channel

Syntax

prohibited-channel [**quiet** *quiet-value*]

undo prohibited-channel

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が禁止されたチャネルのアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 です。デフォルトは 600 秒で

す。WIPS は遅延時間内に禁止されたチャネルを検出してもアラームを引き起こしません。

説明

prohibited-channel コマンドは禁止されたチャネル検出を有効にします。

undo prohibited-channel コマンドは禁止されたチャネル検出を無効にします。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、permit-channel コマンドを使用して許可されたチャネルリストを設定します。

例

禁止されたチャネル検出を有効にします。遅延時間を 100 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] prohibited-channel quiet 100

関連コマンド

- **permit-channel**

2.1.111 random-mac-scan

Syntax

random-mac-scan enable

undo random-mac-scan enable

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

説明

random-mac-scan enable コマンドは、ランダム擬似 MAC アドレスフィルタリング機能を有効にするために使用します。

undo random-mac-scan enable コマンドはデフォルトに戻します。

例

ランダム擬似 MAC アドレス フィルタリングを有効にします。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] random-mac-scan enable

2.1.112 report-interval

Syntax

report-interval *interval*

undo report-interval

デフォルト

30000 ミリ秒

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

interval: センサーが AC に検出した装置の情報を通知する間隔を指定します。設定範囲は 1000～300000 ミリ秒です。

説明

report-interval コマンドはセンサーが AC に検出した装置の情報を通知する間隔を設定します。

undo report-interval コマンドはデフォルトに戻します。

例

センサーが AC に検出した装置の情報を通知する間隔を 10000 ミリ秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] report-interval 10000

2.1.113 reset wips statistics

Syntax

reset wips statistics

View

User view

パラメータ

network-admin

説明

reset wips statistics コマンドはすべてのセンサーから収集した情報を削除します。

例

すべてのセンサーから収集した情報を消去します。

<Sysname> reset wips statistics

関連コマンド

- **display wips statistics receive**

2.1.114 reset wips virtual-security-domain

Syntax

reset wips virtual-security-domain *vsd-name* **device** { **ap** { **all** | **mac-address** *mac-address* } | **client** { **all** | **mac-address** *mac-address* } | **all** }

View

User view

定義済みユーザーロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 装置のエントリを消去します。

ap: AP のエントリを消去します。

all: すべての AP のエントリを消去します。

mac-address *mac-address*: AP のエントリを消去します。mac-address 引数は AP の MAC アドレスをあらわします。

client: クライアントのエントリを消去します。

all: すべてのクライアントのエントリを消去します。

mac-address *mac-address*: クライアントのエントリを消去します。mac-address 引数はクライアントの MAC アドレスをあらわします。

all: すべての AP とクライアントのエントリを消去します。

説明

reset wips virtual-security-domain コマンドは VSD にある学習した AP もしくはクライアントのエントリを削除します。

例

VSD aaa にある学習した AP とクライアントのエントリを消去します。

<Sysname> reset wips virtual-security-domain aaa device all

関連コマンド

- **display wips virtual-security-domain device**

2.1.115 reset wips virtual-security-domain countermeasure record

Syntax

set wips virtual-security-domain *vsd-name* **countermeasure record**

View

User view

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

reset wips virtual-security-domain countermeasure record コマンドは WIPS が不正な装置に対して講じた対策に関する情報を消去します。

例

VSD aaa のために WIPS が不正な装置に対して講じた対策に関する情報を消去します。

<Sysname> reset wips virtual-security-domain aaa countermeasure record

関連コマンド

- **display wips virtual-security-domain countermeasure record**

2.1.116 reset wlan nat-detect

Syntax

reset wlan nat-detect

View

User view

定義済みユーザーロール

network-admin

説明

reset wlan nat-detect コマンドは NAT を設定したクライアントに関する情報を削除します。

例

NAT を構成したクライアントに関する情報をクリアします。

<Sysname> reset wlan nat-detect

関連コマンド

- **display wlan nat-detect**

2.1.117 rssi

Syntax

rssi *value1* [**to** *value2*]

undo rssi

デフォルト

一致なし

View

AP classification rule view

パラメータ

value1 [to *value2*] : 一致する信号強度値の範囲を指定します。*value1* と *value2* は一致する信号強度の値で、範囲は 0 から 100 です。*value2 の値は*、*value1* の値以上である必要があります。

説明

rssi コマンドは、AP 分類ルールで AP 信号の信号強度を一致させるために使用されます。

undo rssi コマンドを使用して、デフォルトに戻します。

例

ID 1 の AP 分類ルールで信号強度が 20 ～ 40 の AP を照合します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] ap-classification rule 1

[Sysname-wips-cls-rule-1] rssi 20 to 40

2.1.118 rssi-change-threshold

Syntax

rssi-change-threshold *threshold-value*

undo rssi-change-threshold

デフォルト

20

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

threshold-value: 装置検出の RSSI 相違のしきい値を指定します。設定範囲は 1～100 です。

説明

rssi-change-threshold コマンドは装置検出の RSSI 相違のしきい値を設定します。

undo rssi-change-threshold コマンドはデフォルトに戻します。

例

装置検出の RSSI 相違のしきい値を 80 に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] rssi-change-threshold 80

2.1.119 rssi-threshold

Syntax

ssi-threshold { **ap** *ap-rssi-value* | **client** *client-rssi-value* }

undo rssi-threshold { **ap** | **client** }

デフォルト

設定なし

View

Attack detection policy view

パラメータ

network-admin

説明

ap *ap-rssi-value*: AP の RSSI しきい値を指定します。設定範囲は 1～100 です。

client *client-rssi-value*: クライアントの RSSI しきい値を指定します。設定範囲は 1～100 です。

説明

rssi-threshold コマンドは装置検出の RSSI しきい値を設定します。

undo rssi-threshold コマンドはデフォルトに戻します。

例

信号強度が 80 を超過している AP を検出するために WIPS を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] rssi-threshold ap 80

2.1.120 security

Syntax

security { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }

undo security

デフォルト

設定なし

View

AP classification rule view

パラメータ

equal: 指定されたセキュリティモードと等しいセキュリティモードと整合します。

include: 指定されたセキュリティモードを含むセキュリティモードと整合します。

clear: 消去するセキュリティモードを指定します。

wep: WEP セキュリティモードを指定します。

wpa: WPA セキュリティモードを指定します。

wpa2: WPA 2 セキュリティモードを指定します。

説明

security コマンドは AP に使用されるセキュリティモードと整合するように AP 分類ルールを設定します。

undo security コマンドはデフォルトに戻します。

例

WEP セキュリティモードを使用する AP と整合するように AP classification rule 1 を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] ap-classification rule 1

[Sysname-wips-cls-rule-1] security equal wep

2.1.121 select sensor all

Syntax

select センサー all

undo select センサー

デフォルト

直近で攻撃者を検出したセンサーのみ、その攻撃者に対して対策を講じます。

View

Countermeasure policy view

定義済みユーザーロール

network-admin

説明

select sensor all コマンドは攻撃者を検出するすべてのセンサーを有効にします。

undo select sensor all コマンドは設定を削除します。

例

攻撃者に対して対策を講じるために、攻撃者を検出するすべてのセンサーを有効にします。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] countermeasure policy home

[Sysname-wips-ctm-home] select sensor all

2.1.122 seq-number

Syntax

seq-number *seq-value1* [**to** *seq-value2*]

undo seq-number

デフォルト

設定なし

View

Signature view

定義済みユーザーロール

network-admin

パラメータ

seq-value1 [*to seq-value2*]: フレームのシーケンス番号の範囲を指定します。seq-value1 引数と seq-value2 引数は、それぞれ値の範囲の始めと終わりを指定します。seq-value1 引数と seq-value2 引数の値の範囲は、どちらも 0～4095 です。ただし、seq-value2 引数の値は seq-value1 引数の値より大きくなければなりません。

説明

seq-number コマンドはシーケンス番号をもつフレームと整合するサブ署名を設定します。

undo seq-number コマンドはデフォルトに戻します。

例

シーケンス番号 100 をもつフレームと整合するサブ署名を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature rule 1

[wips-sig-rule-1] seq-number 100

関連コマンド

- **frame-type**
- **mac-address**
- **ssid-length**
- **ssid (signature rule view)**
- **pattern**
- **match all (signature rule view)**

2.1.123 signature policy

Syntax

signature policy *policy-name*

undo signature policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザーロール

network-admin

パラメータ

policy-name: signature ポリシーの名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

signature policy コマンドは signature ポリシーを作成し、その view に移行します。指定された signature ポリシーがすでに存在する場合、signature policy view に移行します。

undo signature policy コマンドは sigunature ポリシーを削除します。

例

signature ポリシーhome を作成し、その view に移行します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature policy home

2.1.124 signature rule

Syntax

signature rule *rule-id*

undo signature rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザーロール

network-admin

パラメータ

rule-id: signature ID を指定します。範囲は 1～65535 です。

説明

signature rule コマンドは署名を作成し、その view に移行します。指定された署名がすでに存在する場合、signature view に移行します。

undo signature rule コマンドは署名を削除します。

例

signature 1 を作成し、その view に移行します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature rule 1

2.1.125 soft-ap

Syntax

soft-ap [**convert-time** *time-value*]

undo soft-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

convert-time *time-value*: ソフト AP がクライアントと AP の役割を切り替える間隔を指定します。time-value 引数の値の範囲は 5～600 秒です。デフォルト値は 10 秒です。

説明

soft-ap コマンドはソフト AP 検出を有効にします。

undo soft-ap コマンドはソフト AP 検出を無効にします。

例

ソフト AP 検出を有効にします。*time-value* 引数の値を 100 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] soft-ap convert-time 100

2.1.126 ssid (AP classification rule view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*

undo ssid

デフォルト

設定なし

View

AP classification rule view

定義済みユーザーロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

ssid-string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドは AP に対して無線装置の SSID を整合するように AP 分類ルールを設定します。

undo ssid コマンドはデフォルトに戻します。

例

SSID abc の無線サービスを使用した AP を整合するために AP classification rule 1 を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] ap-classification rule 1

[Sysname-wips-cls-rule-1] ssid equal abc

2.1.127 ssid (signature view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *string*

undo ssid

デフォルト

設定なし

View

Signature view

定義済みユーザーロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドはフレームの SSID を整合するためにサブ署名を設定します。

undo ssid コマンドはデフォルトに戻します。

例

signature 1 に対して SSID office のフレームを整合するためにサブ署名を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature rule 1

[Sysname-wips-sig-rule-1] ssid equal office

関連コマンド

- **frame-type**
- **mac-address**
- **seq-number**
- **ssid-length**
- **pattern**
- **match all (signature rule view)**

2.1.128 ssid-length

Syntax

ssid-length *length-value1* [**to** *length-value2*]

undo ssid-length

デフォルト

設定なし

View

Signature rule

定義済みユーザーロール

network-admin

パラメータ

length-value1 [*to length-value2*]: SSID 長の値の範囲を指定します。length-value1 引数と length-value2 引数は、それぞれ値の範囲の始めと終わりを指定します。length-value1 引数と length-value2 引数の値の範囲は、どちらも 1～32 です。ただし、length-value2 引数の値は length-value1 引数の値より大きくなければなりません。

説明

ssid-length コマンドはフレームの SSID 長を整合するためにサブ署名を設定します。

undo ssid-length コマンドはデフォルトに戻します。

例

SSID 長が 10 のフレームを整合するためにサブ署名を設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] signature rule 1

[Sysname-wips-sig-1] ssid-length 10

関連コマンド

- **frame-type**
- **mac-address**
- **seq-number**
- **ssid (signature rule view)**
- **pattern**
- **match all (signature rule view)**

2.1.129 trust mac-address

Syntax

trust mac-address *mac-address*

undo trust mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザーロール

network-admin

パラメータ

mac-address: MAC アドレスを指定します。

all: すべての MAC アドレスを指定します。

説明

trust mac-address コマンドは許可された装置リストに AP もしくはクライアントの MAC アドレスを追加します。

undo trust mac-address コマンドは許可された装置リストから 1 つあるいはすべての MAC アドレスを削除します。

例

許可された装置リストに MAC アドレス 78AC-C0AF-944F を追加します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] classification policy home

[Sysname-wips-cls-home] trust mac-address 78AC-C0AF-944F

2.1.130 trust oui

Syntax

trust oui *oui*

undo trust oui { *oui* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザーロール

network-admin

パラメータ

oui: OUI の名前を指定します。大文字と小文字を区別しません。文字数は 6 文字です。

all: すべての OUI を指定します。

説明

trust oui コマンドは信頼された OUI リストに OUI を追加します。

undo trust oui コマンドは信頼された OUI リストから 1 つあるいはすべての OUI を削除します。

例

信頼された OUI リストに OUI 000fe4 と 000fe5 を追加します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] classification policy home

[Sysname-wips-cls-home] trust oui 000fe4

[Sysname-wips-cls-home] trust oui 000fe5

2.1.131 trust ssid

Syntax

trust ssid *ssid-name*

undo trust ssid { *ssid-name* | **all** }

デフォルト

設定なし

View

Classification policy view

パラメータ

ssid-name: SSID の名前を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

all: すべての SSID を指定します。

説明

trust ssid コマンドは信頼された SSID リストに SSID を追加します。

undo trust ssid コマンドは信頼された SSID リストから 1 つあるいはすべての SSID を削除します。

例

信頼された SSID リストに SSID flood1 を追加します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] classification policy home

[Sysname-wips-cls-home] trust ssid flood1

2.1.132 unencrypted-authorized-ap

Syntax

unencrypted-authorized-ap [**quiet** *quiet-value*]

undo unencrypted-authorized-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可 AP を検出してアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可 AP を検出してもアラームを引き起こしません。

説明

unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を有効にします。

undo unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を無効にします。

例

暗号化されていない許可 AP 検出を有効にします。遅延時間を 10 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] unencrypted-authorized-ap quiet 10

2.1.133 unencrypted-trust-client

Syntax

unencrypted-trust-client [**quiet** *quiet-value*]

undo unencrypted-trust-client

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可クライアントを検出してアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可クライアントを検出してもアラームを引き起こしません。

説明

unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を有効にします。

undo unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を無効にします。

例

暗号化されていない許可クライアント検出を有効にします。遅延時間を 10 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] unencrypted-trust-client quiet 10

2.1.134 up-duration

Syntax

up-duration *value1* [**to** *value2*]

undo up-duration

デフォルト

設定なし

View

AP classification rule view

定義済みユーザーロール

network-admin

パラメータ

value1 [*to value2*]: AP の動作時間の値の範囲を指定します。value1 引数と value2 引数は、それぞれ値の範囲の始めと終わりを指定します。value1 引数と value2 引数の値の範囲は、どちらも 0～2592000 です。ただし、value2 引数の値は value1 引数の値より大きくなければなりません。

説明

up-duration コマンドは AP の動作時間と整合するように AP 分類ルールを設定します。

undo up-duration コマンドはデフォルトに戻します。

例

2000～40000 秒の動作時間の AP と整合するように AP 分類ルールを設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] ap-classification rule 1

[Sysname-wips-cls-rule-1] up-duration 2000 to 40000

2.1.135 virtual-security-domain

Syntax

virtual-security-domain *vsd-name*

undo virtual-security-domain *vsd-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザーロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

virtual-security-domain コマンドは VSD を作成し、その view に移行します。

undo virtual-security-domain コマンドは VSD を削除します。

例

VSD office を作成し、その view に移行します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] virtual-security-domain office

[Sysname-wips-vsd-office]

2.1.136 weak-iv

Syntax

weak-iv [**quiet** *quiet-value*]

undo weak-iv

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がウィーク IV のアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にウィーク IV を検出してもアラームを引き起こしません。

説明

weak-iv コマンドはウィーク IV 検出を有効にします。

undo weak-iv コマンドはデフォルトに戻します。

デバイスが Weak IV を検出すると、警告メッセージが送信されます。

例

ウィーク IV 検出を有効にします。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] weak-iv

2.1.137 windows-bridge

Syntax

windows-bridge [**quiet** *quiet-value*]

undo windows-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Windows ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に Windows ブリッジを検出してもアラームを引き起こしません。

説明

windows-bridge コマンドは Windows ブリッジ検出を有効にします。

undo windows-bridge コマンドは Windows ブリッジを無効にします。

例

Windows ブリッジ検出を有効にします。遅延時間を 360 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] windows-bridge quiet 360

2.1.138 wips (system view)

Syntax

wips

undo wips

デフォルト

設定なし

View

System view

定義済みユーザーロール

network-admin

説明

wips コマンドを使用して、WIPS view に移行します。

undo wips コマンドを使用して、WIPS view のすべての構成を削除します。

例

WIPS view に移行します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips]

2.1.139 wips enable

Syntax

wips enable

undo wips enable

デフォルト

Radio view では、無線が AP group radio view で設定を使用します。

AP group radio view では、WIPS は無効になっています。

View

Radio view

AP group radio view

定義済みユーザーロール

network-admin

説明

wips enable コマンドは WIPS を有効にし、Radio を WISP センサーにします。

undo wips コマンドを使用して、デフォルトに戻します。

無線通信と WIPS センサーは同じ Radio 上での併用をサポートしています。

無線通信と WIPS センサーを併用している Radio の WIPS スキャンは、通信への影響を与えないために、端末との通信のないタイミングで行われます。

また、無線通信と WIPS センサーが有効な Radio に対する通信、および端末の接続に対しては、通信を優先するため WIPS 検出はできません。

例

#AP ap1 の無線 1 に対して WIPS を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1]radio 1

[AP-wlan-ap-ap1-radio-1] wips enable

#AP group apgroup1 のモデル QX-W1020 を持つ AP の無線 1 に対して WIPS を有効にします。

<AC> system-view

[AC]wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020]radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1]wips enable

2.1.140 wips virtual-security-domain

Syntax

wips virtual-security-domain *vsd-name*

undo wips virtual-security-domain

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、AP グループは VSD に追加されません。

View

AP view

AP group view

定義済みユーザーロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

wips virtual-security-domain コマンドは AP を VSD に追加します。

undo wips virtual-security-domain コマンドは AP を VSD から削除します。

例

VSD office に AP を追加します。

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] wips virtual-security-domain office

AP group apgroup1 を VSD office に追加します。

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] wips virtual-security-domain office

2.1.141 wireless-bridge

Syntax

wireless-bridge [**quiet** *quiet-value*]

undo wireless-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザーロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無線ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。quiet-value 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に無線ブリッジを検出してもアラームを引き起こしません。

説明

wireless-bridge コマンドは無線ブリッジ検出を有効にします。

undo wireless-bridge コマンドは無線ブリッジを無効にします。

例

無線ブリッジ検出を有効にします。遅延時間を 100 秒に設定します。

<Sysname> system-view

[Sysname] wips

[Sysname-wips] detect policy home

[Sysname-wips-dtc-home] wireless-bridge quiet 100

2.1.142 wlan nat-detect

Syntax

wlan nat-detect { **disable** | **enable** }

undo wlan nat-detect

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、NAT を設定したクライアントの検出は無効になっています。

View

AP view

AP group view

定義済みユーザーロール

network-admin

説明

wlan nat-detect enable コマンドは NAT を設定したクライアント検出を有効にします。

wlan nat-detect disable コマンドは NAT を設定したクライアント検出を無効にします。

undo wlan nat-detect コマンドを使用して、デフォルトに戻します。

デバイスは、NAT で設定されたクライアントを検出するとアラームを生成します。 検出された NAT 設定クライアントに関する情報を表示するには、display wlan nat-detect コマンドを使用します。

例

AP ap1 用に NAT が設定されているクライアントの検出を有効にします。

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] wlan nat-detect enable

AP group aaa の AP 用に NAT が設定されているクライアントの検出を有効にします。

<Sysname> system-view

[Sysname] wlan ap-group aaa

[Sysname-wlan-ap-group-aaa] wlan nat-detect enable

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

9. 無線管理

本マニュアルは以下に示す章で構成されています。

01-無線管理

02-WLAN 無線ロードバランス

03-WLAN ロードバランス

04-WLAN 無線リソース計測

05-WLAN RRM

06-バンドナビゲーション

07-チャネルスキャン

08-スペクトル管理

目次

このセクションのページは**9-x-x** です。

1 章 無線管理 1-1
1.1 無線管理設定コマンド 1-1
1.1.1 a-mpdu 1-1
1.1.2 a-msdu 1-2
1.1.3 ani 1-3
1.1.4 antenna type 1-4
1.1.5 beacon-interval 1-5
1.1.6 bss-color 1-6
1.1.7 channel 1-7
1.1.8 channel auto-select 1-10
1.1.9 channel band-width 1-12
1.1.10 channel-usage measure 1-16
1.1.11 channel-usage threshold 1-17
1.1.12 client dot11ac-only 1-18
1.1.13 client dot11ax-only 1-19
1.1.14 client dot11b-forbidden 1-20
1.1.15 client dot11n-only 1-21
1.1.16 client max-count 1-23
1.1.17 continuous-mode 1-24
1.1.18 display wlan ap continuous-mode 1-25
1.1.19 display wlan ap radio 1-26
1.1.20 display wlan ap radio channel 1-29
1.1.21 display wlan ap radio type 1-30
1.1.22 display wlan statistics ap radio 1-31
1.1.23 distance 1-40
1.1.24 dl-ofdma 1-41
1.1.25 dot11ac mandatory maximum-nss 1-42
1.1.26 dot11ac multicast-nss 1-44
1.1.27 dot11ac support maximum-nss 1-45
1.1.28 dot11ax mandatory maximum-nss 1-47
1.1.29 dot11ax multicast-nss 1-48
1.1.30 dot11ax support maximum-he-mcs 1-50
1.1.31 dot11ax support maximum-nss 1-51
1.1.32 dot11be mandatory maximum-nss 1-52
1.1.33 dot11be multicast-nss 1-53
1.1.34 dot11be support maximum-nss 1-55

1.1.35 dot11g protection 1-56
1.1.36 dot11n mandatory maximum-mcs 1-57
1.1.37 dot11n multicast-mcs 1-59
1.1.38 dot11n protection 1-60
1.1.39 dot11n support maximum-mcs 1-61
1.1.40 fragment-threshold 1-63
1.1.41 green-energy-management 1-64
1.1.42 ldpc 1-65
1.1.43 long-retry threshold 1-66
1.1.44 max-power 1-67
1.1.45 mru 1-69
1.1.46 mu-txbf 1-70
1.1.47 power-lock 1-72
1.1.48 preamble 1-73
1.1.49 pre-puncture static 1-74
1.1.50 protection-mode 1-75
1.1.51 protection-threshold 1-76
1.1.52 radio 1-77
1.1.53 radio enable 1-78
1.1.54 rate 1-79
1.1.55 reset wlan statistics ap radio 1-81
1.1.56 short-gi 1-82
1.1.57 short-retry threshold 1-83
1.1.58 smart-antenna 1-84
1.1.59 smart-antenna policy 1-85
1.1.60 stbc 1-87
1.1.61 su-txbf 1-88
1.1.62 twt negotiate 1-89
1.1.63 type 1-91
1.1.64 ul-ofdma 1-93
1.1.65 wlan in-band 6g-discovery 1-94
1.1.66 wlan multiple-bssid enable 1-96
1.1.67 wlan out-band 6g-discovery 1-97
1.1.68 wlan radio 1-98

1章 無線管理

1.1 無線管理設定コマンド

1.1.1 a-mpdu

Syntax

a-mpdu { **disable** | **enable** }

undo a-mpdu

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、A-MPDU 機能がオンになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

a-mpdu enable コマンドは、A-MPDU 機能を有効にするために使用します。

a-mpdu disable コマンドは、A-MPDU 機能をオフにするために使用します。

undo a-mpdu コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、または dot11g に切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#A-MPDU 機能をオフにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] a-mpdu disable

#A-MPDU 機能をオフにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] a-mpdu disable

1.1.2 a-msdu

Syntax

a-msdu { **disable** | **enable** }

undo a-msdu

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、A-MSDU 機能がオンになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

a-msdu enable コマンドは、A-MSDU 機能を有効にするために使用します。

a-msdu disable コマンドは、A-MSDU 機能をオフにするために使用します。

undo a-msdu コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、または dot11g に切り替わると、設定はキャンセルされます。

現在、デバイスは A-MSDU メッセージの受信のみをサポートし、A-MSDU の送信はサポートしていません。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#A-MSDU 機能をオフにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] a-msdu disable

#A-MSDU 機能をオフにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] a-msdu disable

1.1.3 ani

Syntax

ani { **disable** | **enable** }

undo ani

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、ANI 機能がオンになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

ani enable コマンドを使用して、ANI (Adaptive Noise Immunity、自動干渉防止)機能をオンにします。

ani disable コマンドを使用して、ANI 機能をオフにします。

undo ani コマンドを使用して、デフォルトの構成を復元します。

ANI 機能をオンにすると、周辺の信号環境に応じてノイズ耐性レベルが自動的に調整され、周辺の無線周波数の干渉を相殺します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#ANI 機能をオンにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] ani enable

#ANI 機能をオンにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] ani enable

1.1.4 antenna type

Syntax

antenna type *antenna-type*

undo antenna type

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、AP モデルに関連して、デバイスの実際の状態を確認します。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

antenna-type:RF アンテナタイプ。1~10 文字の文字列です。サポートされている RF アンテナのタイプは AP モデルに依存します。デバイスの実際の状態に基づいてください。

説明

antenna type コマンドを使用して、無線周波数アンテナタイプを設定します。

undo antenna type コマンドを使用して、デフォルトの状態を復元します。

アンテナタイプを設定すると、送信電力が正しい範囲内に収まるよう、アンテナ利得が自動的に変化します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

アンテナタイプを internal に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] antenna type internal

アンテナタイプを internal に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] antenna type internal

1.1.5 beacon-interval

Syntax

beacon-interval *interval*

undo beacon-interval

デフォルト

Radio view の下で、AP グループ設定を継承します。

AP group's radio view では、Beacon フレームの送信間隔は 100 TU です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

interval:Beacon フレームを送信する時間間隔で、 32～8191 の範囲の値をとり、単位は TU (Time Unit、1 TU=1024 マイクロ秒)。

説明

beacon-interval コマンドは、Beacon フレームを送信する間隔を設定するために使用します。

undo beacon-interval コマンドを使用して、デフォルトの状態を復元します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#Beacon フレームを送信する間隔を 1000 TU に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] beacon-interval 1000

#Beacon フレームを送信する間隔を 1000 TU に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] beacon-interval 1000

1.1.6 bss-color

🕮 **メモ：**

bss-color コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでのみサポートしています。

Syntax

bss-color { **disable** | **enable** }

undo bss-color

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、BSS Color 機能がオンになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

bss-color enable コマンドは、BSS Color 機能を有効にするために使用します。

bss-color disable コマンドは、BSS Color 機能で使用されます。

undo bss-color コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、802.11ax モードと 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、dot11g、dot11n、dot11ac、または dot11gac に切り替わると、設定はキャンセルされます。

BSS Color (BSS color bit、BSS のカラービット)機能は、 AP がメッセージを送信する前に、受信したデータフレーム中に搭載されている BSS Color から、受信したデータメッセージが自分が送信したものかどうかを判断し、自分が送信したものであれば、そのまま退避する。さもなければ、干渉しているとはみなさず、メッセージをそのまま送信する。

AP の密集配置の場面で本機能を起動した後、AP は受信したデータメッセージが自分から来たかどうかを迅速に判断でき、かつ即時にバックオフを行い、システムレベルの性能とチャネルの有効使用率を向上させる。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#BSS Color 機能をオフにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1130

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] bss-color disable

#BSS Color 機能をオフにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1130

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1130-radio-1] bss-color disable

関連コマンド

type dot11ax

1.1.7 channel

Syntax

channel { *channel-number* | **auto** { **lock** | **unlock** } }

undo channel [**auto**]

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、動作チャネルは auto unlock モードです。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

channel-number:手動で設定された RF 動作チャネル。値の範囲は、エリアコードと無線周波数モードによって決まります。

auto lock:チャネルを自動的に選択してロックするモード。デバイスが実際の環境に基づいて最適なチャネルを自動的に選択してロックする。

auto unlock:チャネルを自動的に選択し、モードを解除します。デバイスは、実際の環境に基づいて最適なチャネルを自動的に選択し、ロックなしモードに設定します。

説明

channel コマンドを使用して、無線周波数動作チャネルを設定します。

undo channel コマンドを使用して、デフォルトの状態を復元します。

手動で動作チャネルモードを指定すると、現在の動作チャネルでレーダー信号が検出された場合、AP はすぐに動作チャネルを別のチャネルに調整します。AP は、30 分後に手動で指定されたチャネルに切り替えて、しばらくの間サイレント状態にします。サイレント状態の間にレーダー信号が検出されない場合は、そのチャネルの使用を開始します。レーダー信号が検出されると、再びチャネルが切り替えられる。

自動選択チャネルモードでは、チャネルがロックされているかどうかにかかわらず、現在の動作チャネルでレーダー信号が検出されると、AP は動作チャネルを他のチャネルに直ちに調整する。

AP view の Radio の設定は、AP group view の Radio の設定よりも優先されます。

例

#AP ap1 (QX-W1020) の動作チャネルを 48 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel 48

#AP ap2 (QX-W1120) の動作チャネルを 48 に設定します。

<AC> system-view

[AC] wlan ap ap2 model QX-W1120

[AC-wlan-ap-ap2] radio 1

[AC-wlan-ap-ap2-radio-1] channel 48

#AP ap3 (QX-W1240) の動作チャネルを 48 に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1120

[AC-wlan-ap-ap3] radio 2

[AC-wlan-ap-ap3-radio-2] channel 48

#AP グループ名が apgroup1 で、型番が QX-W1020 である AP の Radio1 の動作チャネルを 48 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel 48

#AP グループ名が apgroup1 で、型番が QX-W1120 である AP の Radio1 の動作チャネルを 48 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1120

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120-radio-1] channel 48

#AP グループ名が apgroup1 で、型番が QX-W1240 である AP の Radio2 の動作チャネルを 48 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1240

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240-radio-2] channel 48

1.1.8 channel auto-select

Syntax

channel auto-select { **blacklist** | **whitelist** } *channel-number*

undo channel auto-select { **blacklist** | **whitelist** } { **all** | *channel-number* }

デフォルト

radio view では、無線は AP group view の設定を使用します。

AP group radio view では、チャネル選択のブラックリストまたはホワイトリストは存在しません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

blacklist：チャネル選択のブラックリストにチャネルを追加します。AP が自動チャネル選択を行うときには、ブラックリストに存在するチャネルは選択されません。

whitelist：チャネル選択のホワイトリストにチャネルを追加します。AP が自動チャネル選択を行う際には、ホワイトリストに存在するチャネルのみ、選択されます。

channel-number：チャネル番号によりチャネルを指定します。この引数の値の範囲は、無線モードにより異なります。

all：ブラックリストに登録されているすべてのチャネルを指定します。

説明

channel auto-select コマンドは、チャネル選択のブラックリストまたはホワイトリストを設定します。

undo channel auto-select コマンドは、ブラックリストまたはホワイトリストから指定したチャネルを削除します。

同じ AP に対して、ブラックリストとホワイトリストの両方にチャネル選択を設定することはできません。どちらかを選択して設定してください。

この機能は、AP が自動チャネル選択モードで動作している場合に限り、有効になります。

例

#AP 名が ap1 (QX-W1020) の Radio 1 のチャネル選択ホワイトリストに、チャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel auto-select whitelist 56 60 64

#AP 名が ap2 (QX-W1120) の Radio 1 のチャネル選択ホワイトリストに、チャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap ap2 model QX-W1120

[AC-wlan-ap-ap2] radio 1

[AC-wlan-ap-ap2-radio-1] channel auto-select whitelist 56 60 64

#AP 名が ap3 (QX-W1240) の Radio 2 のチャネル選択ホワイトリストに、チャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1240

[AC-wlan-ap-ap3] radio 2

[AC-wlan-ap-ap3-radio-2] channel auto-select whitelist 56 60 64

#AP グループ名が apgroup1 で、型番が QX-W1020 である AP の Radio1 のチャネル選択ホワイトリストに、チャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel auto-select whitelist 56 60 64

#AP グループ名が apgroup1 で、型番が QX-W1120 である AP の Radio1 のチャネル選択ホワイトリストに、チャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1120

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120-radio-1] channel auto-select whitelist 56 60 64

#AP グループ名が apgroup1 で、型番が QX-W1240 である AP の Radio2 のチャネル選択ホワイトリストに、チャネル 56、60、64 を追加します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1240

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240-radio-2] channel auto-select whitelist 56 60 64

関連コマンド

channel

1.1.9 channel band-width

Syntax

channel band-width { **20** | **40** [**auto-switch**] | **80** | **160** }

undo channel band-width

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group radio view では、帯域幅モードは 802.11be/eax では 160MHz、802.11ac/ax/abe では 80MHz、802.11an では 40MHz、802.11gac/gax/gbe/gn では 20MHz です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

20：帯域幅モードを 20 MHz に設定します。

40：帯域幅モードを 40 MHz に設定します。

80：帯域幅モードを 80 MHz に設定します。

auto-switch：20 MHz と 40 MHz を自動的に切り替えることができます。このパラメータの設定は、Radio モードが 802.11g、802.11gac、802.11gax にのみ適用されます。

160：帯域幅モードを 160 MHz に設定します。

320：帯域幅モードを 320 MHz に設定します。

🕮 **メモ：**

- 160MHz のパラメータは、QX-W1130 の Radio1、QX-W1200 シリーズの 6GHz および 5GHz の無線でサポートしています。
- 320MHz のパラメータは QX-W1210 と QX-W1230 の Radio1 でサポートしています。

説明

channel band-width コマンドは、帯域幅モードを設定します。

undo channel band-width コマンドは、デフォルト値に戻します。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、802.11gax タイプの Radio に適用可能です。Radio モードを変更すると、帯域幅は変更後の無線モードのデフォルト値に戻ります。

- 40MHz の帯域幅が指定されている場合、結合可能な 2 つの隣接チャネルが見つかった場合、40MHz の帯域幅が使用されます。バインド可能な隣接チャネルが見つからない場合、実際に使用できるのは 20MHz の帯域幅のみです。
- 80MHz の帯域幅が指定されている場合、80MHz にバインドできる隣接チャネルのセットが見つかった場合は、80MHz の帯域幅が使用されます。80 MHz にバインドできるチャネルのセットが見つからないが、40MHz の帯域幅にバインドできる 2 つのチャネルが見つかった場合は、40MHz の帯域幅が使用されます。バインド可能なチャネルが見つからない場合、実際に使用できるのは 20MHz の帯域幅のみです。
- 160MHz の帯域幅が指定されている場合、160MHz にバインドできる隣接チャネルのセットが見つかった場合は、160MHz の帯域幅が使用されます。160MHz にバインドできるチャネルのセットが見つからないが、80MHz にバインドできる隣接チャネルのセットが見つかった場合は、80MHz の帯域幅が使用されます。80MHz にバインドできるチャネルのセットが見つからないが、40MHz の帯域幅にバインドできるチャネルのセットが見つかった場合は、40MHz の帯域幅が使用されます。バインド可能なチャネルが見つからない場合、実際に使用できるのは 20MHz の帯域幅のみです。

プロトコルの規定によれば、無線周波数の実際の動作帯域幅は 2 つに分けられ、そのうち第 1 の帯域幅の位置は主チャネルによって決定され、第 2 の帯域幅の位置は副チャネルによって決定される。メインチャネルはデータフレームとすべての制御、管理フレームを送信するセカンダリチャネルはプライマリチャネルにバンドルされ、データフレームのみを送信します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

帯域幅設定が AP グループを継承する場合、セカンダリチャネルも AP グループを継承しますが、セカンダリチャネルは AP グループを継承しません。

例

AP 名が ap1 (QX-W1020) の Radio 1 の帯域幅を 40 MHz に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] channel band-width 40

This operation might cause channel change. Continue? [Y/N]:y

[AC-wlan-ap-ap1-radio-1]

AP 名が ap2 (QX-W1120) の Radio 1 の帯域幅を 40 MHz に設定します。

<AC> system-view

[AC] wlan ap ap2 model QX-W1120

[AC-wlan-ap-ap2] radio 1

[AC-wlan-ap-ap2-radio-1] type dot11an

[AC-wlan-ap-ap2-radio-1] channel band-width 40

[AC-wlan-ap-ap2-radio-1] This operation might cause channel change. Continue? [Y/N]:y

[AC-wlan-ap-ap2-radio-1]

AP 名が ap3 (QX-W1240) の Radio 2 の帯域幅を 40 MHz に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1240

[AC-wlan-ap-ap3] radio 2

[AC-wlan-ap-ap3-radio-2] type dot11an

[AC-wlan-ap-ap3-radio-2] channel band-width 40

[AC-wlan-ap-ap3-radio-2] This operation might cause channel change. Continue? [Y/N]:y

[AC-wlan-ap-ap3-radio-2]

#AP グループ名が apgroup1 で、型番が QX-W1020 である AP の Radio 1 の帯域幅を 40 MHz に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

This operation might log off all clients. Continue? [Y/N]:y

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel band-width 40

This operation might cause channel change. Continue? [Y/N]:y

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1]

#AP グループ名が apgroup1 で、型番が QX-W1120 である AP の Radio 1 の帯域幅を 40 MHz に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1120

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120-radio-1] type dot11an

This operation might log off all clients. Continue? [Y/N]:y

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120-radio-1] channel band-width 40

This operation might cause channel change. Continue? [Y/N]:y

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1120-radio-1]

#AP グループ名が apgroup1 で、型番が QX-W1240 である AP の Radio 2 の帯域幅を 40 MHz に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1240

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240-radio-2] type dot11an

This operation might log off all clients. Continue? [Y/N]:y

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240-radio-2] channel band-width 40

This operation might cause channel change. Continue? [Y/N]:y

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1240-radio-2]

関連コマンド

channel

1.1.10 channel-usage measure

Syntax

channel-usage measure

View

Radio view

定義済みユーザロール

network-admin

説明

チャネル使用率を測定するには、**channel-usage measure** コマンドを使用します。

チャネル使用率を測定する場合、AP は現在の無線周波数でサポートされているチャネルのリストを取得し、次に、測定のためにチャネルリスト内のチャネルをポーリングし、各チャネルに測定時間を 1 秒間保持します。すべてのチャネルの測定が終了すると、測定結果が表示されます。

例

#チャネル使用率を測定するために ap 1 の Radio 2 を設定して下さい。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] channel-usage measure

```
Please wait......Done.
Channel  Usage
1        63%
2        61%
3        55%
4        45%
5        64%
6        74%
7        66%
8        48%
9        35%
10       38%
11       54%
12       30%
```

```
13      72%
```

1.1.11 channel-usage threshold

Syntax

channel-usage threshold *threshold*

undo channel-usage threshold

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下では、90%です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

threshold:チャネル使用率アラームしきい値をパーセンテージで指定します。値の範囲は 5 から 100 です 。

説明

channel usage threshold コマンドは チャネル使用率アラームしきい値を設定します 。

undo channel usage threshold コマンドはデフォルトに戻します。

チャネル使用率がしきい値を超えると、装置は info center にアラームを報告します。

例

AP ap1 の Radio1 のチャネル使用率アラーム しきい 値を 20% に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel-usage threshold 20

AP グループ 1 の AP の Radio1 のチャネル使用率アラーム しきい 値を 20% に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] channel-usage threshold 20

1.1.12 client dot11ac-only

Syntax

client dot11ac-only { **disable** | **enable** }

undo client dot11ac-only

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下では、802.11ac および 802.11ax クライアントアクセス機能のみがオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

client dot11ac-only enable コマンドを使用して、802.11ac および 802.11ax クライアントのみのアクセスを有効にします。

client dot11ac-only disable コマンドを使用して、802.11ac および 802.11ax クライアントのみのアクセスを許可する機能をオフにします。

undo client dot11ac-only コマンドを使用して、デフォルトの状態を復元します。

この設定は、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効です。Radio モードが切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

802.11 ac および 802.11 ax クライアントのみのアクセスを有効にすると、802.11ac および 802.11 ax クライアントのみがこの Radio にアクセスでき、802.11ac および 802.11ax をサポートしていない無線に関連付けられているクライアントはオフラインになります。

例

#オンにすると、802.11ac および 802.11ax ユーザのみが機能にアクセスできます。(Radio view)

<System> system-view

[System] wlan ap ap1 model QX-W1020

[System-wlan-ap-ap1] radio 1

[System-wlan-ap-ap1-radio-1] type dot11ac

[System-wlan-ap-ap1-radio-1] client dot11ac-only enable

#AP グループでは、802.11ac および 802.11ax のユーザのみが機能にアクセスできます。
(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] client dot11ac-only enable

関連コマンド

- **dot11ac mandatory maximum-nss**

1.1.13 client dot11ax-only

Syntax

client dot11ax-only { **disable** | **enable** }

undo client dot11ax-only

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下では、802.11ax クライアントアクセス機能だけがオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

client dot11ax-only enable コマンドは、802.11ax クライアントのみにアクセスを許可する機能をオンにするために使用します。

client dot11ax-only disable コマンドは、802.11ax クライアントのみのアクセスを許可する機能をオフにするために使用します。

undo client dot11ax-only コマンドを使用して、デフォルトの状態を復元します。

802.11ax クライアントのみのアクセスを有効にすると、802.11ax クライアントのみがこの Radio にアクセスできるようになります。無線に関連付けられているが、802.11ax をサポートしていないクライアントはオフラインになります。

この設定は、802.11ax および 802.11gax モードの Radio でのみ有効です。Radio モードが切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#オンにすると、802.11ax ユーザのみが機能にアクセスできます。(Radio view)

<System> system-view

[System] wlan ap ap1 model QX-W1020

[System-wlan-ap-ap1] radio 1

[System-wlan-ap-ap1-radio-1] type dot11ax

[System-wlan-ap-ap1-radio-1] client dot11ax-only enable

#AP グループでは、802.11ax ユーザのみが機能にアクセスできます。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] client dot11ax-only enable

関連コマンド

- **dot11ax mandatory maximum-nss**

1.1.14 client dot11b-forbidden

Syntax

client dot11b-forbidden { **disable** | **enable** }

undo client dot11b-forbidden

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、802.11b クライアントアクセスを許可して下さい。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

client dot11b-forbidden enable コマンドは、802.11b クライアントのアクセスを無効にするために使用します。

client dot11b-forbidden disable コマンドを使用して、802.11b クライアントにアクセスを許可します。

undo client dot11b-forbidden コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、無線周波数モードが 802.11b、802.11g、802.11gac、802.11gn、802.11gax の場合にのみ設定できます。

ネットワーク転送レートを高め、低レートの 802.11b クライアントの影響を隔離するために、AP は、802.11b クライアントのアクセスを禁止する機能をオンにすることができる。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#設定は 802.11b クライアントアクセスを禁止します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] client dot11b-forbidden enable

#設定は 802.11b クライアントアクセスを禁止します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-model-QX-W1020] radio 2

[AC-wlan-ap-group-apgroup1-model-QX-W1020-radio-2] client dot11b-forbidden enable

1.1.15 client dot11n-only

Syntax

client dot11n-only { **disable** | **enable** }

undo client dot11n-only

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view では、802.11n、802.11ac、および 802.11ax のクライアントアクセス機能のみがオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

client dot11n-only enable コマンドは、802.11n、802.11ac、および 802.11ax クライアントのみを許可する機能をオンにするために使用します。

client dot11n-only disable コマンドは、802.11n、802.11ac、および 802.11ax クライアントのみを許可するアクセス機能をオフにするために使用します。

undo client dot11n-only コマンドを使用して、デフォルトの状態を復元します。

802.11n、802.11ac、および 802.11ax クライアントのみにアクセスを許可する機能を有効にすると、802.11n、802.11ac、および 802.11ax クライアントのみがこの Radio にアクセスできます。802.11n、802.11ac、および 802.11ax をサポートしていない無線に関連付けられたクライアントはオフラインになります。

この設定は、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、または dot11g に切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#オンにすると、802.11n、802.11ac、および 802.11ax クライアントのみが機能にアクセスできます。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] client dot11n-only enable

#オンにすると、802.11n、802.11ac、および 802.11ax クライアントのみが機能にアクセスできます。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client dot11n-only enable

1.1.16 client max-count

Syntax

client max-count *max-number*

undo client max-count

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、無線周波数がアソシエーションを許可するクライアントの最大数を制限しません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

max-number:AP デバイスのモデルに応じた無線周波数で許可されるアソシエーションクライアントの最大数。デバイスの実際の状態に基づいてください。

説明

client max-count コマンドを使用して、無線周波数のアソシエーションを許可するクライアントの最大数を設定します。

undo client max-count コマンドを使用して、デフォルトの状態を復元します。

無線周波数に関連付けられたクライアントの数が、関連付け可能なクライアントの最大数に達すると、新しいクライアントアクセスは受け入れられなくなり、SSID は自動的に非表示になります。

無線周波数で許可されるアソシエーションの最大クライアント数は、AC と AP でそれぞれ制限されるため、同じ無線周波数が AC と AP の両方のワイヤレスサービステンプレートにクライアントアソシエーションの場所をバインドする場合、デバイスで許可されるアソシエーションの最大クライアント数は、設定されているアソシエーションの最大クライアント数の 2 倍になります。このシナリオでは、オンラインになるクライアントの数が必要な場合は、オンラインになるクライアントの予想数に基づいてクライアントの最大数を設定します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#無線周波数の設定アソシエーションを許可するクライアントの最大数は 38 です。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] client max-count 38

#無線周波数の設定アソシエーションを許可するクライアントの最大数は 38 です。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] client max-count 38

関連コマンド

- **client association-location**

1.1.17 continuous-mode

Syntax

continuous-mode { **mcs** *mcs-index* | **nss** *nss-index* **vht-mcs** *vhtmcs-index* | **rate** *rate-value* }

undo continuous-mode

デフォルト

通常モード機能がオフになっています。

View

Radio view

定義済みユーザロール

network-admin

パラメータ

mcs *mcs-index*:通常モードで使用される MCS インデックス値を 0~76 の範囲で指定します。

nss *nss-index*:永続モードで使用される NSS (Number of Spatial Streams、空間ストリーム数)インデックス値を 1~8 の範囲で指定します。

vht-mcs *vhtmcs-index*:永続モードで使用される VHT-MCS インデックス値を 0~9 の範囲で指定します。

rate *rate-value*:通常モードで使用するレートを Mbps で指定します。

説明

continuous-mode コマンドを使用して、無線周波数の通常モード機能をオンにします。

undo continuous-mode コマンドを使用して、デフォルトの状態を復元します。

常時送信モードとは、指定されたレートでパケットを送信し続けてネットワーク環境をテストするもので、テスト専用の機能であり、いったん有効にすると通常の業務に影響を与えるため、ユーザが自分で設定することはお勧めできない。通常モードをオンにした後は、送信電力を調整する以外の操作は推奨されません。

RF モードが 802.11a、802.11b、または 802.11g の場合は、continuous-mode rate rate-value を使用して送信レートを設定します。

RF モードが 802.11n の場合は、continuous-mode rate rate-value を使用して直接送信レートを設定するか、continuous-mode mcs mcs-index を使用して MCS インデックス値を選択して RF レートを指定します。

RF モードが 802.11ac および 802.11gac の場合、continuous-mode rate rate-value を使用して直接送信レートを設定するか、continuous-mode mcs mcs-index を使用して MCS インデックス値を選択して RF レートを指定するか、continuous-mode nss nss-index vht-mcs vhtmcs-index を使用して NSS および MCS インデックス値を選択して RF レートを指定します。

例

#6Mbps の無線周波数の常時送信モード機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] continuous-mode rate 6

関連コマンド

- **display wlan ap continonus-mode**

1.1.18 display wlan ap continuous-mode

Syntax

display wlan ap { **all** | **name** *ap-name* } **continuous-mode**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての AP 無線周波数の通常モードを表示します。

name *ap-name*:指定した AP の無線周波数の標準パターンを表示します。ap-name は AP の名前を示します。1~64 文字の文字列で、英字、数字、アンダースコア、「.」 、[」 、「]、 「/」 、 「-」 を使用でき、大文字と小文字が区別されます。

説明

display wlan ap continuous-mode コマンドを使用して、AP 無線周波数の通常モードを表示します。

例

#ap 1 の Radio の通常モードを表示します。

<AC> display wlan ap name ap1 continuous-mode

```
AP name    Radio ID    Radio type      Rate    Mcs-Index   Nss   Vht-mcs
ap1        1           802.11a         6       N/A         N/A   N/A
```

表 1-1 display wlan ap continuous-mode コマンドの表示情報の説明

フィールド	説明
AP name	AP名
Radio ID	無線ID
Radio type	無線周波数タイプ
Rate	通常モードで使用されるレート
Mcs-Index	通常モードで使用されるMCSインデックス値
Nss	通常モードで使用されるNSSインデックス値
Vht-mcs	通常モードで使用されるVHT-MCSインデックス値

関連コマンド

- **continuous-mode**

1.1.19 display wlan ap radio

Syntax

display wlan ap { **all** | **name** *ap-name* } **radio** [**frequency-band** { **5** | **2.4** }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての AP の無線周波数情報を表示します。

name *ap-name*:指定した AP の無線周波数情報を表示します。ap-name は AP の名前です。1~64 文字の文字列で、英数字、アンダースコア、「.」 、[」 、「]、「/」 、「-」を使用でき、大文字と小文字が区別されます。

radio:AP の無線周波数に関する情報を表示します。

frequency-band:指定した帯域で動作する無線周波数に関する情報を表示します。

5:5 GHz 帯域で動作する無線周波数の情報を表示します。

2.4:2.4 GHz 帯域で動作する無線周波数の情報を表示します。

説明

display wlan ap radio コマンドを使用して、AP の無線周波数情報を表示します。

例

#すべての AP の無線周波数情報を表示します。

<AC> display wlan ap all radio

```
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 6144
Remaining APs: 6144
Total AP licenses: 128
local AP licenses: 0
Server AP licenses: 0
Remaining local AP licenses: 127
Sync AP licenses: 0

AP name               RID State Channel        Usage TxPower Clients
                                                (%)   (dBm)
ap1                   1   Up    149(auto)       10    20     5
```

```
ap1                  2   Up    11(auto)        15     20     10
```

#2.4 GHz 帯域で動作する ap 1 の無線周波数情報を表示します。

<AC> display wlan ap name ap1 radio frequency-band 2.4

```
AP name               RID State Channel        Usage TxPower Clients
                                                (%)   (dBm)
ap1                  2   Up    11(auto)        15     20     15
```

表 1-2 display wlan ap all radio コマンドの表示情報の説明

フィールド	説明
Total number of APs	APの数
Total number of connected APs	接続されているAPの数
Total number of connected manual APs	接続されている手動APの数
Total number of connected auto APs	接続されている自動アクセスポイントの数
Total number of connected common APs	接続されている通常のAPの合計数
Total number of connected WTUs	接続されているWTUの合計数
Total number of inside APs	接続状態の内部アクセスポイント数、内部アクセスポイント数Anchor AP AC機器として自動作成された名前が本製品のMACアドレス、シリアル番号が本製品のシリアル番号である手動アクセスポイント
Maximum supported APs	Fit APおよびWTUを含むAC上のAPの最大容量、WTはAP容量にカウントされない
Remaining APs	APの残りの容量、つまり最大AP容量から接続状態にあるFit APとWTUの数を引いたもの
Total AP licenses	AP license通常のAP Licenseの数を含む合計数、およびWTU Licenseを通常のAP Licenseの数に換算すると、WTU Licenseごとに0.25の通常のAP Licenseに換算されます。
local AP licenses	ACローカルLicense数量
Server AP licenses	ACがサーバから要求したLicenseの数
Remaining local AP licenses	残りのAP licenseの数は、APタイプによって使用されるAP Licenseの数が異なります。たとえば、QX-W1020は1つのAP Licenseを使用し、WT1020はAP Licenseを使用せず、WTU420Hは0.25のAP Licenseを使用します。
Sync AP licenses	共有AP Licenseの数
AP name	AP名
RadioID	無線周波数のID番号

フィールド	説明
State	無線周波数の状態: ● Up:オン ● Down:オフ
Channel	無線周波数使用の動作チャネル
Usage	チャネル使用率
TxPower (dBm)	無線周波数の送信電力(デフォルトは最大電力です)
Clients	オンラインクライアント数

1.1.20 display wlan ap radio channel

Syntax

display wlan ap { **all** | **name** *ap-name* } **radio channel**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての AP の無線周波数チャネル情報を表示します。

name *ap-name*:指定した AP の無線周波数チャネル情報を表示します。ap-name は AP の名前です。1~64 文字の文字列で、英数字、アンダースコア、「.」 、[」 、「]、「/」 、「-」 を使用でき、大文字と小文字が区別されます。

説明

display wlan ap radio channel コマンドを使用して、AP の無線周波数チャネル情報を表示します。

例

#ap 3 の RF チャネル情報を表示します。

<AC> display wlan ap name ap3 radio channel

```
AP name               RID Channel        Band-width         CenterFreq
                                        (MHz)
ap3                   1   36(auto)       20/40/80/160/(80+80) 42/58
ap3                   2   149            20/40/80           155
ap3                   3   11(auto)       20                 0
```

表 1-3 display wlan ap name radio channel コマンドの表示情報の説明

フィールド	説明
AP name	AP名
RID	無線周波数のID番号
Channel	無線周波数使用の動作チャネル
Band-width (MHz)	サポートされるチャネル帯域幅
CenterFreq	帯域幅中心点:サポートされているチャネル帯域幅が80 MHzを超える場合にのみ表示されます。サポートされているチャネルの帯域幅が160/(80+80) MHzに達すると、プライマリチャネルとセカンダリチャネルの両方の中心周波数ポイントが表示されます。

1.1.21 display wlan ap radio type

Syntax

display wlan ap { **all** | **name** *ap-name* } **radio type**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての AP 無線のタイプを表示します。

name *ap-name*:指定した AP 無線のタイプを表示します。ap-name は AP の名前です。1~64 文字の文字列で、英数字、アンダースコア、[」 、 「]、 「/」 、 「-」 を使用でき、大文字と小文字が区別されます。

説明

display wlan ap radio type コマンドを使用して、AP 無線のタイプを表示します。

例

#ap 1 の無線周波数のタイプを表示します。

<AC> display wlan ap name ap1 radio type

```
AP name               RID  AP state  Radio state  Radio type
ap1                   1    Up       Up          802.11n(5GHz)
ap1                   2    Up       Down        802.11n(2.4GHz)
```

表 1-4 display wlan ap radio type コマンドの表示情報の説明

フィールド	説明
AP name	AP名
RID	無線周波数のID番号
AP state	APステータス: ● Up:APとACの間でCAPWAPトンネルが正常に確立されました。 ● Down:APがACとCAPWAPトンネルを確立していません
Radio state	● 無線周波数の状態: ● Up:無線周波数がオンになっています ● Down:無線周波数がオフになっています
Radio type	無線周波数タイプ

1.1.22 display wlan statistics ap radio

Syntax

display wlan statistics ap { **all** | **name** *ap-name* } **radio**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての AP の無線周波数統計情報を表示します。

ap *ap-name*:指定した AP の無線周波数統計情報を表示します。ap-name は AP の名前を表し、1~64 文字の文字列で、大文字と小文字が区別されます。

説明

display wlan statistics ap radio コマンドを使用して、無線周波数の統計情報を表示します。

例

#ap 1 の無線周波数統計情報を表示します。

```
<AC> display wlan statistics ap name ap1 radio
                            Radio statistics
--------------------------------------------------------------------------
---
```

```
 AP name:ap1                                Radio ID:1
-------------------------------------------------------------------------------
---
Transmitted frame statistics:
   Total frames                            :836532
   Total frame bytes                        :214040681
   Unicast frames                          :4
   Unicast frame bytes                      :900
   Broadcast/Multicast frames               :836528
   Broadcast/Multicast frame bytes          :214039781
   Other frames                            :0
   Other frame bytes                        :0

   Discarded frames                        :0
   Failed RTS frames                        :0
   Retransmissions                         :6
   Successful RTS frames                    :0
   Retransmitted frames                     :3
   No-ACK frames                           :1555
   Authentication frames                    :1
   Association frames                       :1

   Packet statistics by size:
     Smaller than or equal to 128           :747
     Between 128 and 512 (inclusive)        :85983
     Between 512 and 1024 (inclusive)       :0
     Larger than 1024                      :0

   Packet statistics by rate:
      1 Mbps  :0          2 Mbps  :0
    5.5 Mbps  :0          6 Mbps  :0
      9 Mbps  :0         11 Mbps  :0
     12 Mbps  :0         18 Mbps  :0
     24 Mbps  :880       36 Mbps  :0
     48 Mbps  :0         54 Mbps  :0

  Packet statistics based on data rate:
    6.5 Mbps  :0           7.2 Mbps  :0
     13 Mbps  :0          13.5 Mbps  :0
   14.4 Mbps  :0            15 Mbps  :0
   19.5 Mbps  :0          21.7 Mbps  :0
     26 Mbps  :0            27 Mbps  :0
   28.9 Mbps  :0          29.3 Mbps  :0
```

```
     30 Mbps  :0          32.5 Mbps  :0
     39 Mbps  :0          40.5 Mbps  :0
   43.3 Mbps  :0            45 Mbps  :0
     52 Mbps  :0            54 Mbps  :0
   57.8 Mbps  :0          58.5 Mbps  :0
     60 Mbps  :0            65 Mbps  :0
   72.2 Mbps  :0            78 Mbps  :1
     81 Mbps  :0          86.7 Mbps  :0
   87.8 Mbps  :0            90 Mbps  :0
   97.5 Mbps  :0           104 Mbps  :3
    108 Mbps  :0         115.6 Mbps  :0
    117 Mbps  :0           120 Mbps  :0
  121.5 Mbps  :0           130 Mbps  :0
    135 Mbps  :0         144.4 Mbps  :0
    150 Mbps  :0           156 Mbps  :0
    162 Mbps  :0         173.3 Mbps  :0
  175.5 Mbps  :0           180 Mbps  :0
    195 Mbps  :0           200 Mbps  :0
    216 Mbps  :0         216.7 Mbps  :0
    234 Mbps  :0           240 Mbps  :0
    243 Mbps  :0           260 Mbps  :0
  263.3 Mbps  :0           270 Mbps  :0
  288.9 Mbps  :0         292.5 Mbps  :0
    300 Mbps  :0           324 Mbps  :0
    325 Mbps  :0           351 Mbps  :0
    360 Mbps  :0         364.5 Mbps  :0
    390 Mbps  :0           400 Mbps  :0
    405 Mbps  :0         433.3 Mbps  :0
    450 Mbps  :0           468 Mbps  :0
    486 Mbps  :0           520 Mbps  :0
  526.5 Mbps  :0           540 Mbps  :0
    585 Mbps  :0           600 Mbps  :0
    650 Mbps  :0           702 Mbps  :0
    780 Mbps  :0         866.7 Mbps  :0
  877.5 Mbps  :0           975 Mbps  :0
   1053 Mbps  :0          1170 Mbps  :0
   1300 Mbps  :0
-------------------------------------------------------------------------------
---
Received frame statistics:
   Total frames                    :420815
   Total frame bytes                :24112652
   Unicast frames                   :585
```

```
Unicast frame bytes               :15357
Broadcast/Multicast frames         :420230
Broadcast/Multicast frame bytes     :24097295
Fragmented frames                 :0
Duplicate frames                  :0
FCS failures                     :474471639
Decryption errors                 :0
Authentication frames              :1
Association frames                :1

Packet statistics by size:
  Smaller than or equal to 128          :420759
  Between 128 and 512 (inclusive)        :54
  Between 512 and 1024 (inclusive)       :0
  Larger than 1024                    :0

Packet statistics by rate:
    6 Mbps  :420115      9 Mbps  :0
   12 Mbps  :0          18 Mbps  :0
   24 Mbps  :0          36 Mbps  :1
   48 Mbps  :0          54 Mbps  :2

Packet statistics based on data rate:
  6.5 Mbps  :0           7.2 Mbps  :0
   13 Mbps  :0          13.5 Mbps  :0
 14.4 Mbps  :0            15 Mbps  :0
 19.5 Mbps  :0          21.7 Mbps  :0
   26 Mbps  :0            27 Mbps  :0
 28.9 Mbps  :0          29.3 Mbps  :0
   30 Mbps  :0          32.5 Mbps  :0
   39 Mbps  :0          40.5 Mbps  :0
 43.3 Mbps  :0            45 Mbps  :0
   52 Mbps  :1            54 Mbps  :2
 57.8 Mbps  :0          58.5 Mbps  :17
   60 Mbps  :0            65 Mbps  :10
 72.2 Mbps  :0            78 Mbps  :48
   81 Mbps  :0          86.7 Mbps  :70
 87.8 Mbps  :0            90 Mbps  :0
 97.5 Mbps  :0           104 Mbps  :87
  108 Mbps  :0         115.6 Mbps  :170
  117 Mbps  :130         120 Mbps  :0
121.5 Mbps  :0           130 Mbps  :140
  135 Mbps  :0         144.4 Mbps  :22
```

```
    150 Mbps  :0           156 Mbps  :0
    162 Mbps  :0         173.3 Mbps  :0
  175.5 Mbps  :0           180 Mbps  :0
    195 Mbps  :0           200 Mbps  :0
    216 Mbps  :0         216.7 Mbps  :0
    234 Mbps  :0           240 Mbps  :0
    243 Mbps  :0           260 Mbps  :0
  263.3 Mbps  :0           270 Mbps  :0
  288.9 Mbps  :0         292.5 Mbps  :0
    300 Mbps  :0           324 Mbps  :0
    325 Mbps  :0           351 Mbps  :0
    360 Mbps  :0         364.5 Mbps  :0
    390 Mbps  :0           400 Mbps  :0
    405 Mbps  :0         433.3 Mbps  :0
    450 Mbps  :0           468 Mbps  :0
    486 Mbps  :0           520 Mbps  :0
  526.5 Mbps  :0           540 Mbps  :0
    585 Mbps  :0           600 Mbps  :0
    650 Mbps  :0           702 Mbps  :0
    780 Mbps  :0         866.7 Mbps  :0
  877.5 Mbps  :0           975 Mbps  :0
   1053 Mbps  :0          1170 Mbps  :0
   1300 Mbps  :0
--------------------------------------------------------------------------------
---
                            Radio statistics
--------------------------------------------------------------------------------
---
 AP name:ap1                                Radio ID:2
--------------------------------------------------------------------------------
---
Transmitted frame statistics:
  Total frames                          :13134
  Total frame bytes                      :3259997
  Unicast frames                        :11
  Unicast frame bytes                    :3518
  Broadcast/Multicast frames             :13123
  Broadcast/Multicast frame bytes         :3256479
  Other frames                          :0
  Other frame bytes                      :0

  Discarded frames                      :0
  Failed RTS frames                     :0
```

```
 Retransmissions                        :58
 Successful RTS frames                   :0
 Retransmitted frames                    :11
 No-ACK frames                          :7541
 Authentication frames                   :14
 Association frames                      :8

 Packet statistics by size:
   Smaller than or equal to 128          :1020
   Between 128 and 512 (inclusive)       :11386
   Between 512 and 1024 (inclusive)      :0
   Larger than 1024                      :0

 Packet statistics by rate:
     1 Mbps  :0          2 Mbps  :0
   5.5 Mbps  :0          6 Mbps  :0
     9 Mbps  :0         11 Mbps  :1121
    12 Mbps  :0         18 Mbps  :0
    24 Mbps  :0         36 Mbps  :0
    48 Mbps  :0         54 Mbps  :0

Packet statistics based on data rate:
  6.5 Mbps  :3           7.2 Mbps  :0
   13 Mbps  :1          13.5 Mbps  :0
 14.4 Mbps  :0            15 Mbps  :0
 19.5 Mbps  :4          21.7 Mbps  :0
   26 Mbps  :0            27 Mbps  :0
 28.9 Mbps  :0          29.3 Mbps  :0
   30 Mbps  :0          32.5 Mbps  :0
   39 Mbps  :1          40.5 Mbps  :0
 43.3 Mbps  :0            45 Mbps  :0
   52 Mbps  :0            54 Mbps  :0
 57.8 Mbps  :0          58.5 Mbps  :0
   60 Mbps  :0            65 Mbps  :0
 72.2 Mbps  :0            78 Mbps  :0
   81 Mbps  :0          86.7 Mbps  :0
 87.8 Mbps  :0            90 Mbps  :0
 97.5 Mbps  :0           104 Mbps  :1
  108 Mbps  :0         115.6 Mbps  :0
  117 Mbps  :1           120 Mbps  :0
121.5 Mbps  :0           130 Mbps  :0
  135 Mbps  :0         144.4 Mbps  :0
  150 Mbps  :0           156 Mbps  :0
```

```
    162 Mbps  :0          173.3 Mbps  :0
  175.5 Mbps  :0            180 Mbps  :0
    195 Mbps  :0            200 Mbps  :0
    216 Mbps  :0          216.7 Mbps  :0
    234 Mbps  :0            240 Mbps  :0
    243 Mbps  :0            260 Mbps  :0
  263.3 Mbps  :0            270 Mbps  :0
  288.9 Mbps  :0          292.5 Mbps  :0
    300 Mbps  :0            324 Mbps  :0
    325 Mbps  :0            351 Mbps  :0
    360 Mbps  :0          364.5 Mbps  :0
    390 Mbps  :0            400 Mbps  :0
    405 Mbps  :0          433.3 Mbps  :0
    450 Mbps  :0            468 Mbps  :0
    486 Mbps  :0            520 Mbps  :0
  526.5 Mbps  :0            540 Mbps  :0
    585 Mbps  :0            600 Mbps  :0
    650 Mbps  :0            702 Mbps  :0
    780 Mbps  :0          866.7 Mbps  :0
  877.5 Mbps  :0            975 Mbps  :0
   1053 Mbps  :0           1170 Mbps  :0
   1300 Mbps  :0
-------------------------------------------------------------------------------
---
Received frame statistics:
   Total frames                      :32156
   Total frame bytes                  :3076192
   Unicast frames                    :1613
   Unicast frame bytes                :102957
   Broadcast/Multicast frames          :30543
   Broadcast/Multicast frame bytes     :2973235
   Fragmented frames                 :0
   Duplicate frames                  :2
   FCS failures                      :9978084
   Decryption errors                 :0
   Authentication frames              :14
   Association frames                :8

   Packet statistics by size:
     Smaller than or equal to 128          :25327
     Between 128 and 512 (inclusive)        :6097
     Between 512 and 1024 (inclusive)       :0
     Larger than 1024                    :0
```

```
Packet statistics by rate:
    1 Mbps  :28718       2 Mbps  :1895
  5.5 Mbps  :284         6 Mbps  :29
    9 Mbps  :12         11 Mbps  :0
   12 Mbps  :10         18 Mbps  :24
   24 Mbps  :11         36 Mbps  :5
   48 Mbps  :4          54 Mbps  :0

Packet statistics based on data rate:
  6.5 Mbps  :45              7.2 Mbps  :0
   13 Mbps  :53             13.5 Mbps  :0
 14.4 Mbps  :0                15 Mbps  :0
 19.5 Mbps  :120            21.7 Mbps  :0
   26 Mbps  :136              27 Mbps  :0
 28.9 Mbps  :0              29.3 Mbps  :0
   30 Mbps  :0              32.5 Mbps  :0
   39 Mbps  :59             40.5 Mbps  :0
 43.3 Mbps  :0                45 Mbps  :0
   52 Mbps  :17               54 Mbps  :0
 57.8 Mbps  :0              58.5 Mbps  :20
   60 Mbps  :0                65 Mbps  :4
 72.2 Mbps  :0                78 Mbps  :0
   81 Mbps  :0              86.7 Mbps  :0
 87.8 Mbps  :0                90 Mbps  :0
 97.5 Mbps  :0               104 Mbps  :0
  108 Mbps  :0             115.6 Mbps  :0
  117 Mbps  :0               120 Mbps  :0
121.5 Mbps  :0               130 Mbps  :0
  135 Mbps  :0             144.4 Mbps  :0
  150 Mbps  :0               156 Mbps  :0
  162 Mbps  :0             173.3 Mbps  :0
175.5 Mbps  :0               180 Mbps  :0
  195 Mbps  :0               200 Mbps  :0
  216 Mbps  :0             216.7 Mbps  :0
  234 Mbps  :0               240 Mbps  :0
  243 Mbps  :0               260 Mbps  :0
263.3 Mbps  :0               270 Mbps  :0
288.9 Mbps  :0             292.5 Mbps  :0
  300 Mbps  :0               324 Mbps  :0
  325 Mbps  :0               351 Mbps  :0
  360 Mbps  :0             364.5 Mbps  :0
  390 Mbps  :0               400 Mbps  :0
```

```
  405 Mbps  :0              433.3 Mbps  :0
  450 Mbps  :0                468 Mbps  :0
  486 Mbps  :0                520 Mbps  :0
526.5 Mbps  :0                540 Mbps  :0
  585 Mbps  :0                600 Mbps  :0
  650 Mbps  :0                702 Mbps  :0
  780 Mbps  :0              866.7 Mbps  :0
877.5 Mbps  :0                975 Mbps  :0
 1053 Mbps  :0               1170 Mbps  :0
 1300 Mbps  :0
--------------------------------------------------------------------------------
----
```

表 1-5 display wlan statistics ap radio コマンドの各フィールドの説明

フィールド	説明
AP name	アクセスポイント名
Radio ID	無線ID番号
Transmitted frame statistics	転送されたフレームの統計
Total frames	Probe ResponseおよびBeaconフレームを含む、送信されたフレームの合計数
Total frame bytes	Probe ResponseおよびBeaconフレームを含む、送信フレームの合計バイト数
Unicast frames	Probe Responseフレームを除く、送信されたユニキャストフレームの総数
Unicast frame bytes	Probe Responseフレームを除く、送信されたユニキャストフレームの合計バイト数
Broadcast/Multicast frames	Beaconフレームを除く、送信されたブロードキャスト/マルチキャストフレームの合計数
Broadcast/Multicast frame bytes	Beaconフレームを除く、送信されたブロードキャスト/マルチキャストフレームの合計バイト数
Others frames	送信された他のフレームの合計数
Other frame bytes	送信された他のフレームの合計バイト数
Discarded frames	破棄されたフレームの数
Failed RTS frames	送信に失敗したRTSフレームの数
Retransmissions	再送が発生した回数
Successful RTS frames	送信に成功したRTSフレームの数
Retransmitted frames	再送フレーム数
No-ACK frames	ACKメッセージを受信しなかった送信フレームの数
Authentication frames	送信された認証フレームの数
Association frames	転送された関連フレームの数
Packet statistics by size	メッセージサイズごとにメッセージ数をカウントする
Packet statistics by rate	802.11a/b/gのレートでのメッセージ数

フィールド	説明
Packet statistics based on data rate	802.11nのレートでメッセージ数をカウントします。デバイスが802.11nをサポートしていない場合、カウントは表示されません。
Received frame statistics	受信フレームの統計
Total frames	受信したフレームの合計数
Total frame bytes	受信フレームの合計バイト数
Unicast frames	受信したユニキャストフレームの総数
Unicast frame bytes	受信したユニキャストフレームの合計バイト数
Broadcast/Multicast frames	受信したブロードキャスト/マルチキャストフレームの合計数
Broadcast/Multicast frame bytes	受信したブロードキャスト/マルチキャストフレームの合計バイト数
Fragmented frames	受信されたタイルフレームの数
Duplicate frames	受信した繰り返しフレームの数
FCS failures	受信中にFCSエラーが発生したフレームの数
Decryption errors	受信中にデコードエラーが発生したフレームの数
Authentication frames	受信した認証フレームの数
Association frames	受信した関連フレームの数

1.1.23 distance

Syntax

distance *distance*

undo distance

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view では、無線周波数でカバーできる最大距離は 1 km です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

distance:無線周波数が到達可能な最大距離。1~40 km の範囲で値を指定できます。

説明

distance コマンドを使用して、無線周波数が到達可能な最大距離を設定します。

undo distance コマンドを使用して、デフォルトの状態を復元します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#無線周波数が到達可能な最大距離を 5 km に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] distance 5

#無線周波数が到達可能な最大距離を 5 km に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] distance 5

1.1.24 dl-ofdma

🕮 **メモ：**

dl-ofdma コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでサポートしています。

Syntax

dl-ofdma { **disable** | **enable** }

undo dl-ofdma

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、ダウンストリーム OFDMA 機能はオンになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

dl-ofdma enable コマンドを使用して、ダウンストリーム OFDMA (Orthogonal Frequency Division Multiple Access、直交周波数分割多元接続)機能を有効にします。

dl-ofdma disable コマンドは、ダウンストリーム OFDMA 機能をオフにするために使用します。

undo dl-ofdma コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、802.11ax モードと 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、dot11g、dot11n、dot11ac、または dot11gac に切り替わると、設定はキャンセルされます。

802.11ax は、同じチャネル帯域幅で複数のユーザを多重化する OFDMA の技術を利用している。

アクセス端末が密集し、かつ伝送パケットが比較的小さい場面で本機能を起動した後、AP は同時に複数の無線クライアントにメッセージを伝送することができ、マルチユーザの競争バックオフによる空き時間遅延を大幅に減少させ、空き時間効率を向上させる。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#ダウンストリーム OFDMA 機能をオフにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] dl-ofdma disable

#ダウンストリーム OFDMA 機能をオフにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dl-ofdma disable

関連コマンド

- **type dot11ax**

1.1.25 dot11ac mandatory maximum-nss

Syntax

dot11ac mandatory maximum-nss *nss-number*

undo dot11ac mandatory maximum-nss

デフォルト

Radio view で、802.11ac の最大サポート NSS が構成されている場合、802.11ac の最大ベース NSS はデフォルトで構成されません。802.11ac の最大サポート NSS が設定されていない場合は、デフォルトで AP グループ構成が継承されます。

AP group's radio view の下で、802.11ac のための最大基本 NSS は設定されません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

nss-number:最大ベース NSS。範囲は 1~8 です。

説明

dot11ac mandatory maximum-nss コマンドを使用して、802.11ac の最大ベース NSS を設定します。

undo dot11ac mandatory maximum-nss コマンドを使用して、デフォルトの状態を復元します。

このコマンドで指定された 802.11ac の最大ベース NSS は、dot11ac support maximum-nss コマンドで設定された 802.11ac の最大サポート NSS を超えることはできません。

この設定を変更すると、その無線に現在関連付けられているが、変更された最大ベース NSS をサポートしていないクライアントがオフラインになります。

このコマンドは、802.11ac モードおよび 802.11gac モードの Radio でのみ有効です。Radio モードが dot11ac 以外に切り替わると、設定はキャンセルされます。

例

#802.11ac の基本 NSS の最大値を 7 に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] dot11ac mandatory maximum-nss 7

#802.11ac のための最大基本 NSS を設定して下さい。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11ac

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac mandatory maximum-nss 7

関連コマンド

- **dot11ac support maximum-nss**

1.1.26 dot11ac multicast-nss

Syntax

dot11ac multicast-nss *nss-number* **vht-mcs** *index*

undo dot11ac multicast-nss

デフォルト

Radio view で、802.11ac の最大ベース NSS または最大サポート NSS が設定されている場合、802.11ac のマルチキャスト NSS および VHT-MCS インデックスはデフォルトで設定されず、802.11ac の最大ベース NSS および最大サポート NSS が設定されていない場合、AP グループ設定がデフォルトで継承されます。

AP group's radio view の下で、802.11ac マルチキャスト NSS および VHT-MCS インデックスは設定されません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

nss-number:802.11ac マルチキャスト NSS を 1~8 の範囲の値で指定します。

index:NSS の VHT-MCS インデックス値。範囲は 0~9 です。

説明

dot11ac multicast-nss コマンドは 802.11ac マルチキャスト NSS および VHT-MCS インデックス値を設定するのに使用されます。

undo dot11ac multicast-nss コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定するには、**dot11ac mandatory maximum-nss** コマンドを設定する必要があります。

このコマンドで指定された 802.11ac マルチキャストの NSS は、**dot11ac mandatory maximum-nss** コマンドで設定された 802.11ac の最大ベース NSS を超えることはできません。

このコマンドは、802.11ac モードおよび 802.11gac モードの Radio でのみ有効です。Radio モードが dot11ac 以外に切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#最大基本 NSS を 2 に設定し、マルチキャスト NSS を 2 に設定し、マルチキャスト VHT-MCS インデックスを 2 に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] dot11ac mandatory maximum-nss 2

[AC-wlan-ap-ap1-radio-1] dot11ac multicast-nss 2 vht-mcs 2

#最大基本 NSS を 2 に設定し、マルチキャスト NSS を 2 に設定し、マルチキャスト VHT-MCS インデックスを 2 に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac mandatory maximum-nss 2

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac multicast-nss 2 vht-mcs 2

関連コマンド

- **dot11ac mandatory maximum-nss**

1.1.27 dot11ac support maximum-nss

Syntax

dot11ac support maximum-nss *nss-number*

undo dot11ac support maximum-nss

デフォルト

Radio view では、802.11ac の最大ベース NSS が設定されている場合、802.11ac の最大サポート NSS はデフォルトで 8 になり、802.11ac の最大ベース NSS が設定されていない場合、デフォルトで AP グループ設定が継承されます。

AP group's radio view の下で、802.11ac の最大サポート NSS は 8 です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

nss-number:802.11ac でサポートされる最大 NSS を 1~8 の範囲で指定します。

説明

dot11ac support maximum-nss コマンドを使用して、802.11ac の最大サポート NSS を設定します。

undo dot11ac support maximum-nss コマンドを使用して、デフォルトの状態を復元します。

このコマンドで指定されている 802.11ac の最大サポート NSS は、**dot11ac mandatory maximum-nss** コマンドで設定されている 802.11ac の最大ベース NSS を下回ることはできません。

このコマンドは、802.11ac モードおよび 802.11gac モードの Radio でのみ有効です。Radio モードが dot11ac 以外に切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#802.11ac の最大サポート NSS を 7 に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ac

[AC-wlan-ap-ap1-radio-1] dot11ac support maximum-nss 7

#802.11ac の最大サポート NSS を 7 に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11ac

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ac support maximum-nss 7

関連コマンド

- **dot11ac mandatory maximum-nss**

1.1.28 dot11ax mandatory maximum-nss

Syntax

dot11ax mandatory maximum-nss *nss-number*

undo dot11ax mandatory maximum-nss

デフォルト

Radio view で、802.11ax の最大サポート NSS が構成されている場合、デフォルトでは、802.11ax の最大ベース NSS は構成されません。802.11ax の最大サポート NSS が設定されていない場合、デフォルトで AP グループ構成が継承されます。

AP group's radio view の下で、802.11ax のための最大基本 NSS は設定されません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

nss-number:最大ベース NSS。範囲は 1~8 です。

説明

dot11ax mandatory maximum-nss コマンドを使用して、802.11ax の必須の最大ベース NSS を設定します。

undo dot11ax mandatory maximum-nss コマンドを使用して、デフォルトの状態を復元します。

この設定は、802.11ax および 802.11gax モードの Radio でのみ有効です。Radio モードが切り替わると、設定はキャンセルされます。

AC デバイスでは、Radio view の設定は、AP グループの Radio view の設定よりも優先されます。

このコマンドで指定された 802.11ax の最大ベース NSS は、**dot11ax support maximum-nss** コマンドで設定された 802.11ax の最大サポート NSS を超えることはできません。

このコマンドは、802.11ax モードと 802.11gax モードの Radio でのみ有効です。Radio モードが dot11ax 以外に切り替わると、設定はキャンセルされます。

例

#設定 802.11ax の最大基本 NSS は 8 です。(Radio view)

<System> system-view

[System] wlan ap ap1 model QX-W1020

[System-wlan-ap-ap1] radio 1

[System-wlan-ap-ap1-radio-1] type dot11ax

[System-wlan-ap-ap1-radio-1] dot11ax mandatory maximum-nss 8

#802.11ax の最大基本 NSS を設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ax mandatory maximum-nss 8

関連コマンド

- **type dot11ax**

1.1.29 dot11ax multicast-nss

Syntax

dot11ax multicast-nss *nss-number* **he-mcs** *index*

undo dot11ax multicast-nss

デフォルト

Radio view で、802.11ax の最大ベース NSS または最大サポート NSS が設定されている場合、802.11ax のマルチキャスト NSS および HE-MCS インデックスはデフォルトで設定されず、802.11ax の最大ベース NSS および最大サポート NSS が設定されていない場合、AP グループ設定がデフォルトで継承されます。

AP group's radio view の下で、802.11ax マルチキャスト NSS および HE-MCS インデックスは設定されません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

nss-number:802.11ax マルチキャスト NSS を 1~8 の値の範囲で指定します。

index:NSS の HE-MCS インデックス値。範囲は 0~11 です。

説明

dot11ax multicast-nss コマンドは、802.11ax マルチキャスト NSS と HE-MCS インデックス値を設定します。

undo dot11ax multicast-nss コマンドを使用して、デフォルトの状態を復元します。

このコマンドを設定するには、**dot11ax mandatory maximum-nss** コマンドを設定する必要があります。

このコマンドで指定された 802.11ax マルチキャストの NSS は、**dot11ax mandatory maximum-nss** コマンドで設定された 802.11ax の最大ベース NSS を超えることはできません。

このコマンドは、802.11ax モードと 802.11gax モードの Radio でのみ有効です。Radio モードが dot11ax 以外に切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#最大基本 NSS を 2 に設定し、マルチキャスト NSS を 2 に設定し、マルチキャスト HE-MCS インデックスを 2 に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] dot11ax mandatory maximum-nss 2

[AC-wlan-ap-ap1-radio-1] dot11ax multicast-nss 2 he-mcs 2

#最大基本 NSS を 2 に設定し、マルチキャスト NSS を 2 に設定し、マルチキャスト HE-MCS インデックスを 2 に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ax mandatory maximum-nss 2

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ax multicast-nss 2 he-mcs 2

関連コマンド

- **dot11ax mandatory maximum-nss**

1.1.30 dot11ax support maximum-he-mcs

Syntax

dot11ax support maximum-he-mcs *he-mcs-munber*

undo dot11ax support maximum-he-mcs

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

he-mcs number : 802.11ax でサポートされる HE-MCS の最大値を指定します。使用可能なオプションは 7 、 9 、 11 です。

説明

dot11ax support maximum-he-mc コマンドは 802.11ax でサポートされる HE-MCS の最大値を設定します。

undo dot11ax support maximum-he-mcs コマンド は デフォルトに戻します。

この機能は、802.11ax 無線でのみ有効です。このコマンドはテンプレートで実行し、テンプレートを 802.11ax 無線にバインドすることにより、ワイヤレスサービステンプレートで有効になります。

802.11ax ネットワークでは、ネットワークの品質が悪い場合、ネットワークデバイスが

中程度または低レートで通信するために、802.11ax でサポートされる HE-MCS の最大値を減らすことができます。これにより、高速レートと低速レートの間で頻繁にレート

が変更されることによる通信遅延やジッターを回避できます。

このコマンドで指定されたサポートされる最大 HE-MCS と無線でサポートされる最大 HE-MCS が一致しない場合は、低い方が有効になります。

例

802.11ax でサポートされる HE-MCS の最大値を 7 に設定します。

<AC> system-view

[AC] wlan service-template st

[AC-wlan-st-st] dot11ax support maximum-he-mcs 7

関連コマンド

- **type dot11ax**

1.1.31 dot11ax support maximum-nss

Syntax

dot11ax support maximum-nss *nss-number*

undo dot11ax support maximum-nss

デフォルト

Radio view では、802.11ax の最大ベース NSS が設定されている場合、802.11ax の最大サポート NSS はデフォルトで 8 になり、802.11ax の最大ベース NSS が設定されていない場合、デフォルトで AP グループ構成が継承されます。

AP group's radio view では、802.11ax の最大サポート NSS は 8 です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

nss-number:802.11ax プロトコルのデフォルトのベース NSS の最大値は 1~8 です。

説明

dot11ax support maximum-nss コマンドを使用して、802.11ax の最大サポート NSS を設定します。

undo dot11ax support maximum-nss コマンドを使用して、デフォルトの状態を復元します。

この設定は、802.11ax および 802.11gax モードの Radio でのみ有効です。Radio モードが切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#基本的な NSS の最大サポートは 8 です。(Radio view)

<System> system-view

[System] wlan ap ap1 model QX-W1020

[System-wlan-ap-ap1] radio 1

[System-wlan-ap-ap1-radio-1] type dot11ax

[System-wlan-ap-ap1-radio-1] dot11ax support maximum-nss 8

#AP グループでは、8 までの基本 NSS をサポートするように設定されています。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] dot11ax support maximum-nss 8

関連コマンド

- **type dot11ax**

1.1.32 dot11be mandatory maximum-nss

Syntax

dot11be mandatory maximum-nss *nss-number*

undo dot11be mandatory maximum-nss

デフォルト

Radio view の下で、サポートされる最大 NSS が設定されている場合、最大必須 NSS は設定されません。サポートされる最大 NSS が設定されていない場合、無線は AP group's radio view の設定を使用します。

AP group's radio view で、最大必須 NSS は設定されません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

nss-number:最大必須 NSS を 1~8 の範囲で指定します。

説明

802.11be の最大必須 NSS を設定するには、**dot11be mandatory maximum-nss** を使用します。

デフォルトに戻すには、**undo dot11be mandatory maximum-nss** を使用します。

この設定は、802.11gbe、802.11abe、および 802.11be 無線でのみ有効です。無線モードが切り替わった場合、この設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

802.11be 用にこのコマンドで指定された最大必須 NSS は、802.11be 用の **dot11be support maximum-nss** コマンドで設定された最大サポート NSS を超えることはできません。

例

radio view で最大必須 NSS を 8 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11be

[AC-wlan-ap-ap1-radio-1] dot11be mandatory maximum-nss 8

AP group's radio view で最大必須 NSS を 8 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1240

[AC-wlan-ap-group-1-ap-model-QX-W1240] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1240-radio-1] dot11be mandatory maximum-nss 8

1.1.33 dot11be multicast-nss

Syntax

dot11be multicast-nss *nss-number* **eht-mcs** *index*

undo dot11be multicast-nss

デフォルト

Radio view のデフォルト設定は次のとおりです。

- サポートされる最大 NSS または必須の最大 NSS が設定されている場合、マルチキャスト NSS は設定されません。
- サポートされる最大 NSS も必須の最大 NSS も設定されていない場合、無線は AP group's radio view の設定を使用します。

AP group's radio view では、802.11ax 無線にマルチキャスト NSS は設定されません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

nss-number: 802.11be のマルチキャスト NSS を 1~8 の範囲で指定します。

index:NSS の EHT-MCS インデックスを 0~13 の範囲で指定します。

説明

dot11be multicast-nss を使用して、802.11be のマルチキャスト NSS および EHT-MCS を設定します。

undo dot11be multicast-nss を使用して、デフォルトに戻します。

このコマンドを設定する前に、**dot11be mandatory maximum-nss** コマンドを設定する必要があります。

このコマンドで指定する 802.11be マルチキャストの NSS は、**dot11be mandatory maximum-nss** コマンドで 802.11be に設定されている最大必須 NSS を超えることはできません。

このコマンドは、802.11gbe、802.11abe、および 802.11be 無線でのみ有効です。無線モードを非 dot11be モードに変更すると、この設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

radio view で最大必須 NSS を 2 に、マルチキャスト NSS を 2 に、マルチキャスト EHT-MCS インデックスを 2 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11be

[AC-wlan-ap-ap1-radio-1] dot11be mandatory maximum-nss 2

[AC-wlan-ap-ap1-radio-1] dot11be multicast-nss 2 eht-mcs 2

AP group's radio view で最大必須 NSS を 2 に、マルチキャスト NSS を 2 に、マルチキャスト EHT-MCS インデックスを 2 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1240

[AC-wlan-ap-group-1-ap-model-QX-W1240] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1240-radio-1] dot11be mandatory maximum-nss 2

[AC-wlan-ap-group-1-ap-model-QX-W1240-radio-1] dot11be multicast-nss 2 eht-mcs 2

1.1.34 dot11be support maximum-nss

Syntax

dot11be support maximum-nss *nss-number*

undo dot11be support maximum-nss

デフォルト

Radio view の下で、デフォルト設定は次のとおりです。

- 最大必須 NSS が設定されている場合、サポートされる最大 NSS は 8 です。
- 最大必須 NSS が設定されていない場合、無線は AP group's radio view の設定を使用します。

AP group's radio view でサポートされる最大 NSS は 8 です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

nss-number:802.11be でサポートされる最大 NSS を 1~8 の範囲で指定します。

説明

dot11be support maximum-nss を使用して、802.11be でサポートされる最大 NSS を設定します。

undo dot11be support maximum-nss を使用して、デフォルトに戻します。

このコマンドは、802.11gbe、802.11abe、および 802.11be 無線でのみ有効です。無線モードが変更されると、この設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

AP の radio view で最大 NSS を 8 に設定します。

<ACAC> system-view

[ACAC] wlan ap ap1 model QX-W1240

[ACAC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] dot11be support maximum-nss 8

AP group's radio view で最大 NSS を 8 に設定します。

<ACAC> system-view

[ACAC] wlan ap-group 1

[ACAC-wlan-ap-group-1] ap-model QX-W1240

[ACAC-wlan-ap-group-1-ap-model-QX-W1240] radio 1

[ACAC-wlan-ap-group-1-ap-model-QX-W1240-radio-1] dot11be support maximum-nss 8

1.1.35 dot11g protection

🕮 **メモ：**

ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアから 802.11gbe の無線タイプでの使用をサポートしています。

Syntax

dot11g protection { **disable** | **enable** }

undo dot11g protection

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、802.11g 保護機能がオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

dot11g protection enable コマンドは、802.11g 保護機能を有効にします。

dot11g protection disable コマンドは、802.11g 保護機能を無効にします。

undo dot11g protection コマンドはデフォルトに戻します。

802.11g 保護機能の設定は、無線タイプが 802.11g、802.11n(2.4 GHz)、802.11gac、802.11gax、802.11gbe の場合にのみサポートされます。802.11g 保護機能の設定は、無線タイプを別のタイプに切り替えると削除されます。

802.11g 保護機能を有効にすると、AP が動作チャネルで 802.11b 信号をスキャンした場合、データを送信する前に RTS/CTS メッセージまたは CTS-to-self メッセージを送信して競合を回避し、802.11g 保護機能を開始するようにクライアントに通知します。802.11b 信号が検出されなければ、上記動作は行われない。

802.11b クライアントが 802.11g、802.11n(2.4GHz)、802.11gac、802.11gax、802.11gbe がオンになっている AP 無線にアクセスすると、AP の 802.11g 保護機能が自動的にオンになり、有効になります。

Radio view の下の設定は、AP group's radio view の下の Radio view の下の設定よりも優先されます。

例

#802.11g 保護機能を有効にする。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] type dot11gn

[AC-wlan-ap-ap1-radio-2] dot11g protection enable

#802.11g 保護機能を有効にする。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] type dot11gn

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] dot11g protection enable

関連コマンド

- **protection-mode**

1.1.36 dot11n mandatory maximum-mcs

Syntax

dot11n mandatory maximum-mcs *index*

undo dot11n mandatory maximum-mcs

デフォルト

Radio view では、最大サポート MCS インデックスが構成されている場合、デフォルトで 802.11n のベース MCS インデックスは構成されず、最大サポート MCS インデックスが構成されていない場合、デフォルトで AP グループ構成が継承されます。

AP group's radio view で、802.11n の基本 MCS インデックスが設定されていません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

index:802.11n 無線周波数の最大ベース MCS インデックス値を 0~76 の範囲で指定します。

説明

dot11n mandatory maximum-mcs コマンドを使用して、802.11n 無線の最大基本 MCS インデックスを設定します。

undo dot11n mandatory maximum-mcs コマンドを使用して、デフォルトの状態を復元します。

ユーザが Radio を指定して **dot11n multicast-mcs** コマンドを設定する必要がある場合は、802.11n ベース MCS インデックスの最大数を設定する必要があります。

この設定を変更すると、その RF に現在関連付けられているが、変更されたベース MCS インデックスの最大数をサポートしていないクライアントがオフラインになります。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、または dot11g に切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#無線周波数 802.11n の設定最大基本 MCS インデックスは 14 です。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n mandatory maximum-mcs 14

#無線周波数 802.11n の設定最大基本 MCS インデックスは 14 です。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n mandatory maximum-mcs 14

1.1.37 dot11n multicast-mcs

Syntax

dot11n multicast-mcs *index*

undo dot11n multicast-mcs

デフォルト

Radio view では、最大ベース MCS インデックスまたは最大サポート MCS インデックスが設定されている場合、802.11n のマルチキャスト MCS インデックスはデフォルトで設定されず、最大ベース MCS インデックスと最大サポート MCS インデックスが設定されていない場合、AP グループの設定がデフォルトで継承されます。

AP group's radio view で、802.11n マルチキャスト MCS インデックスが設定されていません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

index:無線周波数 802.11n マルチキャスト MCS インデックス値を 0~76 の範囲で指定します。

説明

dot11n multicast-mcs コマンドを使用して、無線周波数 802.11n のマルチキャスト MCS インデックスを設定します。

undo dot11n multicast-mcs コマンドを使用して、デフォルトの状態を復元します。

マルチキャスト MCS インデックスは、アクセスするクライアントが 802.11n、802.11ac、および 802.11ax クライアントの場合にのみ有効です。

802.11a/b/g クライアントが存在する場合は、ベースモードのマルチキャストレート、つまり 802.11a/b/g のマルチキャストレートのみを選択できます。

マルチキャスト MCS ケーブルが動作する場合は、帯域幅モードが 20MHz モードか 40MHz モードかにかかわらず、20MHz モードに対応したレートに統一する。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、または dot11g に切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#RF 802.11n マルチキャスト MCS インデックスを 14 に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n mandatory maximum-mcs 15

[AC-wlan-ap-ap1-radio-1] dot11n multicast-mcs 14

#RF 802.11n マルチキャスト MCS インデックスを 14 に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n mandatory maximum-mcs 14

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n multicast-mcs 14

1.1.38 dot11n protection

メモ:

ソフトウェアバージョン9.6.05c を含む以降のソフトウェアから802.11abe と 802.11gbe の無線タイプでの使用をサポートしています。

Syntax

dot11n protection { **disable** | **enable** }

undo dot11n protection

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、802.11n 保護機能がオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

dot11n protection enable コマンドは、802.11n 保護機能を有効にします。

dot11n protection disable コマンドを使用して、802.11n 保護機能をオフにします。

undo dot11n protection コマンドを使用して、デフォルトの状態を復元します。

802.11 n 保護機能の設定は、無線周波数モードが 802.11n、802.11ac、802.11gac、802.11ax、802.11gax、802.11abe、802.11gbe である場合にのみサポートされ、無線周波数モードを別のモードに切り替えると、802.11n 保護機能の設定は削除されます。

802.11n 保護機能が有効になっている場合、AP が動作チャネルで 802.11a/b/g 信号をスキャンすると、802.11n 保護機能の開始がクライアントに通知されます。802.11a/b/g 信号が検出されなければ、上記の動作は行われない。

802.11n、802.11ac、802.11gac、802.11ax、802.11gax、802.11abe、802.11gbe の無線タイプが設定された無線に 802.11a/b/g クライアントがアクセスすると、AP の 802.11n 保護機能が自動的に有効になります。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#802.11n 保護機能を有効にする。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] dot11n protection enable

#802.11n 保護機能を有効にする。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n protection enable

1.1.39 dot11n support maximum-mcs

Syntax

dot11n support maximum-mcs *index*

undo dot11n support maximum-mcs

デフォルト

Radio view では、最大ベース MCS インデックスが構成されている場合、802.11n の最大サポート MCS インデックスはデフォルトで 76 になり、最大ベース MCS インデックスが構成されていない場合、デフォルトで AP グループ構成が継承されます。

AP group's radio view では、802.11n でサポートされる MCS インデックスの最大値は 76 です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

index:無線周波数 802.11n の最大サポート MCS インデックス値を 0~76 の範囲で指定します。

説明

dot11n support maximum-mcs コマンドを使用して、無線周波数 802.11n の最大サポート MCS インデックスを設定します。

undo dot11n support maximum-mcs コマンドを使用して、デフォルトの状態を復元します。

このコマンドで指定された 802.11n の最大サポート MCS インデックスは、**dot11n mandatory maximum-mcs** コマンドで設定された 802.11 n の最大基本 MCS インデックスより小さくすることはできません。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、または dot11g に切り替わると、設定はキャンセルされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#無線周波数 802.11n の設定最大サポート MCS インデックスは 14 です。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[System-wlan-ap-ap1-radio-1] dot11n support maximum-mcs 14

#無線周波数 802.11n の設定最大サポート MCS インデックスは 14 です。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] dot11n support maximum-mcs 14

1.1.40 fragment-threshold

Syntax

fragment-threshold *size*

undo fragment-threshold

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view では、フレームのシャードしきい値は 2346 バイトです。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

size:フレームのスライスしきい値。256~2346 の範囲の偶数をバイト単位で取ります。

説明

fragment-threshold コマンドを使用して、フレームのシャードしきい値を設定します。

undo fragment-threshold コマンドを使用して、デフォルトの状態を復元します。

フレームのシャードとは、1 つの大きなフレームを複数の小さなシャードに分割し、各シャードが個別に送信および確認応答を行うことです。フレームの実際のサイズがこの設定で指定されたシャードしきい値を超えると、そのフレームはシャードされます。

干渉が大きい無線ネットワーク環境では、フレームのシャードしきい値を適切に下げ、フレームのシャード数を増やし、デバイスは正常に送信されなかったシャードを再送信するだけでよく、ip mtu コマンドを使用して IP メッセージをシャードし、MTU のしきい値はフレームのシャードしきい値より小さく、スループットを向上させることをお勧めします。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#設定フレームのシャードしきい値は 2048 バイトです。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] fragment-threshold 2048

#設定フレームのシャードしきい値は 2048 バイトです。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] fragment-threshold 2048

1.1.41 green-energy-management

Syntax

green-energy-management { **disable** | **enable** }

undo green-energy-management

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、AP のグリーン電力節約機能がオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

green-energy-management enable コマンドを使用して、AP のグリーン電力節約機能をオンにします。

green-energy-management disable コマンドを使用して、AP のグリーン電力節約機能をオフにします。

undo green-energy-management コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、または dot11g に切り替わると、設定はキャンセルされます。

AP の緑色の省電力機能をオンにすると、Radio に関連付けられているユーザがおらず、Radio で WIPS 機能がオンになっていない場合は、Radio が 1 x 1 モードで動作し、輻射を低減して電力消費を節約します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#AP の省電力機能をオンにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] green-energy-management enable

#AP の省電力機能をオンにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] green-energy-management enable

1.1.42 ldpc

Syntax

ldpc { **disable** | **enable** }

undo ldpc

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、LDPC 機能がオンになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

ldpc enable コマンドを使用して、LDPC 機能をオンにします。

ldpc disable コマンドを使用して、LDPC 機能をオフにします。

undo ldpc コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効です。Radio モードが dot11a、dot11b、または dot11g に切り替わると、設定はキャンセルされます。

現在、デバイスは LDPC メッセージの受信のみをサポートしており、LDPC メッセージの送信はサポートしていません。

802.11ax モードでは、ldpc がサポートされている必要があります。つまり、ldpc disable が設定されていると、802.11ax モードでは動作しません。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#LDPC 機能をオフにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] ldpc disable

#LDPC 機能をオフにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] ldpc disable

1.1.43 long-retry threshold

Syntax

long-retry threshold *count*

undo long-retry threshold

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view では、長いフレームのハードウェア再送信の最大回数は 4 です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

count:長フレームのハードウェア再送信の最大回数。範囲は 1~15 です。

説明

long-retry threshold コマンドを使用して、長いフレームのハードウェア再送信の最大回数を設定します。

undo long-retry threshold コマンドを使用して、デフォルトの状態を復元します。

このコマンドを使用して、フレーム長が RTS しきい値を超えるフレームのハードウェア再送信の最大回数を設定します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#長いフレームのハードウェア再送信の最大数を 5 に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] long-retry threshold 5

#長いフレームのハードウェア再送信の最大数を 5 に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] long-retry threshold 5

関連コマンド

- **protection-threshold**
- **short-retry threshold**

1.1.44 max-power

Syntax

max-power *radio-power*

undo max-power

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、無線周波数はサポートされる最大電力を使用します。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

radio-power:無線周波数の最大送信電力は、エリアコード、チャネル、AP モデル、無線周波数モード、アンテナタイプ、帯域幅などの属性によって決まります。

説明

max-power コマンドを使用して、無線周波数の最大送信電力を設定します。

undo max-power コマンドを使用して、デフォルトの状態を復元します。

無線周波数の最大送信電力は、無線周波数がサポートする電力の範囲内でのみ選択でき、無線周波数の最大送信電力が合法的な範囲内であることを保証します。無線周波数サポートの電力範囲はエリアコード、チャネル、AP モデル、無線周波数モード、アンテナタイプ、帯域幅などの属性によって決定され、前記属性を修正し、無線周波数サポートの電力範囲と最大伝送電力は自動的に合法値に調整される。

RF の電力ロックがオンになっている場合、AC は RF の最大送信電力を RF の現在の送信電力に変更します。

このコマンドを設定すると、現在の Radio の自動電力調整機能は無効になります。自動電力調整機能の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*9 無線管理*”の”*6 章 WLAN RRM*”を参照してください。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#RF の最大送信電力を 15 dBm に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] max-power 15

#無線周波数の最大送信電力を 15 dBm に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] max-power 15

1.1.45 mru

🕮 **メモ：**

mru コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

mru { **disable** | **enable** }

undo mru

デフォルト

radio view：無効

View

Radio view

定義済みユーザロール

network-admin

パラメータ

disable: Multiple Resource Unit (MRU)を無効にします。

enable: Multiple Resource Unit (MRU)を有効にします。

説明

mru enable コマンドは Multiple Resource Unit (MRU)を有効にします。

mru disable コマンドは Multiple Resource Unit (MRU)を無効にします。

undo mru コマンドはデフォルトに戻します。

Multiple Resource Unit (MRU) は、マルチユーザシナリオにおいて、スペクトルリソースの使用率を向上させるために使用される手法です。

従来は、各ユーザが使用できるリソースユニット (RU) は 1 つのみでした。

MRU の機能により、ユーザは複数の RU を使用できます。同じ帯域幅で、1 つの STA が同時に複数の RU リソースを占有できるため、スペクトルリソースの使用率が向上し、通信遅延が削減されます。

このコマンドは Radio type が 802.11be、802.11abe、802.11gbe の無線でのみ使用することができます。Radio type が 802.11be、802.11abe、802.11gbe 以外のモードに切り替わると、このコマンドは無効になります。

例

AP **ap1** で、MRU を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11abe

[AC-wlan-ap-ap1-radio-1] mru enable

1.1.46 mu-txbf

Syntax

mu-txbf { **disable** | **enable** }

undo mu-txbf

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、マルチユーザ TxBF 機能がオンになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

🕮 **メモ** :

このコマンドのサポートは、AP デバイスのモデルによって異なります。デバイスの実際の状態に基づいてください。

mu-txbf enable コマンドは、AP のマルチユーザ TxBF (Tx Beamforming,固定送信波速度成形)機能を有効にするために使用されます。

mu-txbf disable コマンドは、AP のマルチユーザ TxBF 機能をオフにするために使用されます。

undo mu-txbf コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、802.11ac、802.11gac、802.11ax、および 802.11gax モードの Radio でのみ有効で、Radio モードが dot11a、dot11b、dot11g、dot11n モードに切り替わると設定がキャンセルされます。

TxBF 機能をオンにすると、AP はクライアントとの間のチャネル情報を取得することによって、無線周波数エネルギーがクライアントの位置に集中するように信号送信のパラメータを調整し、クライアントが受信する信号品質を向上させる。

マルチユーザ TxBF 技術とは、 AP が TxBF 技術によって複数のクライアントに同時刻にデータを送信し、並列データ転送を提供する技術である。マルチユーザ TxBF は 802.11ac wave2 の一部です。マルチユーザ TxBF 機能をオンにした後、AP は複数のアンテナによって同時に複数のクライアントに無線信号を送信し、チャネル状態情報に基づいて信号送信のパラメータを調整し、特定のクライアントへの情報が他のクライアントに到着する時に信号が最小または感知できないようにする。クライアント間の競合トランスポートのレイテンシーを削減し、情報スループットと AP 帯域幅の使用率を向上させます。この機能は、クライアントの数が多く、AP 帯域幅の使用率と伝送遅延の要件が高い環境に適しています。

マルチユーザ TxBF 機能を有効にするには、まず **su-txbf enable** コマンドを使用してシングルユーザ TxBF 機能を有効にします。

AP 無線がマルチユーザ TxBF 機能を実装できないように、AP 無線のデフォルト MIMO 構成を変更しないことをお勧めします。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#AP マルチユーザ TxBF 機能をオンにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] su-txbf enable

[AC-wlan-ap-ap1-radio-1] mu-txbf enable

#AP マルチユーザ TxBF 機能をオンにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] su-txbf enable

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] mu-txbf enable

関連コマンド

- **su-txbf**

1.1.47 power-lock

Syntax

power-lock { **disable** | **enable** }

undo power-lock

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、電力ロック機能がオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

power-lock enable コマンドを使用して、電力ロック機能をオンにします。

power-lock disable コマンドを使用して、電力ロック機能をオフにします。

undo power-lock コマンドを使用して、デフォルトの状態を復元します。

電力ロックがオンになると、AC は AP の現在の送信電力をロックし、無線周波数の最大送信電力を現在の送信電力に変更します。AC が再起動すると、AP は AC との接続を再確立した後も、ロックされた送信電力を使用し続けます。

電力をロックすると、チャネルが調整され、ロックされた電力値が調整されたチャネルでサポートされる最大電力より大きい場合、デバイスは電力値をチャネルでサポートされる最大電力に調整します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#ロックアウト電力を設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] power-lock enable

#ロックアウト電力を設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] power-lock enable

1.1.48 preamble

Syntax

preamble { **long** | **short** }

undo preamble

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、Radio は短いプリアンブルを使用します。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

long:長いプリアンブル。ネットワーク内に以前のクライアント NIC を使用しているクライアントがある場合は、長いプリアンブルを選択して互換性を持たせることができます。

short:短いプリアンブル。ネットワーク同期のパフォーマンスを向上させるには、短いプリアンブルを選択します。

説明

preamble コマンドを使用して、プリアンブルタイプを設定します。

undo preamble コマンドを使用して、デフォルトの状態を復元します。

プリアンブルはパケットの先頭に位置するビットの組であり、受信者はこれに応じてデータを同期して受信する準備ができる。

設定プリアンブルタイプは、無線周波数モードが 802.11b、802.11g、または 802.11gn の場合にのみサポートされます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#設定プリアンブルの種類は長いプリアンブルです。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] type dot11g

[AC-wlan-ap-ap1-radio-2] preamble long

#設定プリアンブルの種類は長いプリアンブルです。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] type dot11g

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] preamble long

1.1.49 pre-puncture static

🕮 **メモ：**

pre-puncture static コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

pre-puncture static { **disable** | **enable** }

undo pre-puncture static

デフォルト

radio view：無効

View

Radio view

定義済みユーザロール

network-admin

パラメータ

disable: Preamble puncturing を無効にします。

enable: Preamble puncturing を有効にします。

説明

pre-puncture static enable コマンドは Preamble puncturing を有効にします。

pre-puncture static disable コマンドは Preamble puncturing を無効にします。

undo pre-puncture static コマンドはデフォルトに戻します。

本コマンドを使用すると、非連続チャネルを使用したデータ通信が可能になることによって、チャネル干渉を防ぎ、チャネルの使用効率が向上します。

このコマンドは、80MHz 帯、160MHz 帯でのみ適用できます。

このコマンドは、802.11be、802.11gbe、および 802.11abe でのみ有効にすることができます。Radio type が他のモードに切り替わると、このコマンドは無効になります。

例

AP **ap1** で、Preamble puncturing を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] type dot11abe

[AC-wlan-ap-ap1-radio-2] pre-puncture static enable

1.1.50 protection-mode

Syntax

protection-mode { **cts-to-self** | **rts-cts** }

undo protection-mode

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view では、競合回避方法は CTS-to-self です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

cts-to-self:競合回避方法を CTS-to-self に指定します。

rts-cts:競合回避方法を RTS/CTS に指定します。

説明

protection-mode コマンドを使用して、競合回避方法を設定します。

undo protection-mode コマンドを使用して、デフォルトの状態を復元します。

競合回避には、次の 2 つの方法があります。

- RTS/CTS (Request to Send/Clear to Send、送信要求/送信許可)方式:AP があるクライアントにデータを送信するとき、 AP はクライアントに RTS メッセージを送信し、クライアントは RTS を受信すると CTS メッセージを返信し、RTS または CTS メッセージを受信した無線デバイスは指定された時間内にデータ送信を停止する。
- CTS-to-self (リバーシブル CTS)方式:AP はあるクライアントにデータを送信する際、自身の MAC アドレスを宛先 MAC アドレスとして CTS メッセージを送信し、CTS-to-self メッセージを受信した無線は指定された時間データ送信を停止する。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#競合回避方法を RTS/CTS に設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] protection-mode rts-cts

#競合回避方法を RTS/CTS に設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 2

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-2] protection-mode rts-cts

関連コマンド

- **dot11g protection**
- **protection-threshold**

1.1.51 protection-threshold

Syntax

protection-threshold *size*

undo protection-threshold

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view では、RTS しきい値は 2346 バイトです。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

size:RTS しきい値。バイト単位で 0~2346 の値をとります。

説明

RTS しきい値を設定するには、**protection-threshold** コマンドを使用します。

undo protection-threshold コマンドを使用して、デフォルトの状態を復元します。

AP が送信しようとするフレームの長さが RTS 閾値に達した場合、まず衝突回避を実行する必要があり、すなわち RTS/CTS フレームまたは CTS-to-self フレームを使用して伝送領域を空にし、チャネル使用権を取得する。長さが RTS しきい値未満であれば、そのまま送信できる。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#RTS しきい値を 2048 バイトに設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] protection-threshold 2048

#RTS しきい値を 2048 バイトに設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] protection-threshold 2048

関連コマンド

- **protection-mode**

1.1.52 radio

Syntax

radio *radio-id*

View

AP view

AP group’s AP model view

定義済みユーザロール

network-admin

パラメータ

radio-id:RF 番号。このパラメータの範囲は AP モデルに依存します。デバイスの実際の状態に基づいてください。

説明

radio コマンドは、Radio view にアクセスするために使用します。

例

#Radio view に移動します。(AP view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1]

#AP group’s radio view に入ります。(AP group’s view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1]

1.1.53 radio enable

Syntax

radio { **disable** | **enable** }

undo radio

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group’s radio view で、無線周波数がオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

radio enable コマンドを使用して、無線周波数機能をオンにします。

radio disable コマンドは、無線周波数機能をオフにします。

undo radio コマンドを使用して、デフォルトの状態を復元します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#無線周波数をオンにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] radio enable

#無線周波数をオンにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] radio enable

1.1.54 rate

Syntax

rate { **multicast** { **auto** | *rate-value* } | { **disabled** | **mandatory** | **supported** } *rate-value* }

undo rate

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下:

- 802.11a/802.11an/802.11ac/802.11ax:
  - 無効レート:なし。
  - 強制レート:6, 12, 24。
  - マルチキャストレート:強制レートから適切なレートを自動的に選択します。
  - サポート速度:9、18、36、48、54。

- 802.11b:
  - 無効レート:なし。
  - 強制レート:1, 2。
  - マルチキャストレート:強制レートから適切なレートを自動的に選択します。
  - サポート速度:5.5、11。
- 802.11g/802.11gn/802.11gac/802.11gax:
  - 無効レート:なし。
  - 強制レート:1、2、5.5、11。
  - マルチキャストレート:強制レートから適切なレートを自動的に選択します。
  - サポート速度:6、9、12、18、24、36、48、54。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

disabled:レートを無効にします。AP がディセーブルになっているレート。

mandatory:レートを強制します。クライアントが AP を関連付けるとき、AP はクライアントがサポートする必要があるレートを必要とします。

multicast:マルチキャストレート:AP がクライアントにマルチキャストメッセージを送信するレート。マルチキャストレートは強制レートで選択する必要があります。

supported:サポートレート。AP がサポートするレート。クライアントが AP にアソシエートすると、AP がサポートする「サポート・レート・セット」で、より高い/低いレートでメッセージを送信できます。

auto:強制レートから適切なレートをマルチキャストレートとして自動的に選択します。

rate-value:Mbps 単位のレート値。複数のレートをスペースで区切って設定できます。

- 802.11a/802.11an/802.11ac/802.11ax:6、9、12、18、24、36、48、54 の値を使用できます。
- 802.11b:1、2、5.5、11 の値を使用できます。
- 802.11g/802.1gn/802.11gac/802.11gax:1、2、5.5、6、9、11、12、18、24、36、48、54 の値を使用できます。

説明

rate コマンドを使用して、無線周波数レートを設定します。

undo rate コマンドを使用して、デフォルトの状態を復元します。

マルチキャストレートは [強制レート] で選択する必要があり、1 つのレート値のみを設定するか、AP によって適切なレートが自動的に選択されます。

強制レートおよびマルチキャストレートは設定する必要があります。強制レートに値が 1 つしかない場合、ユーザはサポートレートまたはディセーブルレートにこの値を設定できません。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#6 Mbps、12 Mbps、24 Mbps の強制レートを設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rate mandatory 6 12 24

#6 Mbps、12 Mbps、24 Mbps の強制レートを設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] rate mandatory 6 12 24

1.1.55 reset wlan statistics ap radio

Syntax

reset wlan statistics ap { all | name *ap-name* **} radio**

View

User view

定義済みユーザロール

network-admin

パラメータ

all:すべての AP を指定します。

name *ap-name*:AP を名前で指定します。1 文字から 64 文字の大文字と小文字が区別されます。文字列には、文字、数字、アンダースコア (_) 、ドット (。) 、左括弧 ([) 、右括弧 (()]) 、スラッシュ (/) 、ハイフン (-) を使用できます。

説明

reset wlan statistics ap radio コマンドは無線統計情報をクリアします。

例

AP ap1 の無線統計情報をクリアします。

<AC> reset wlan statistics ap name ap1 radio

1.1.56 short-gi

Syntax

short-gi { disable | enable }

undo short-gi

デフォルト

Radio view では、無線は AP group's radio view の設定を使用します。

AP group's radio view では、有効です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

short-gi enable コマンドは short Guard Interval (GI) を有効にします。

short-gi disable コマンドは short GI を無効にします。

undo short-gi コマンドはデフォルトに戻します。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax 無線にのみ適用できます。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

AP ap1 のショート GI を無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] short-gi disable

AP グループ apgroup1 の short GI を無効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] short-gi disable

1.1.57 short-retry threshold

Syntax

short-retry threshold *count*

undo short-retry threshold

デフォルト

Radio view では、無線は AP group's radio view の設定を使用します。

AP group's radio view では、小さいフレームのハードウェア再送信制限は 7 です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

count:小さいフレームのハードウェア再送信制限を 1 から 15 の範囲で指定します。

説明

short-retry threshold コマンドは小さいフレームのハードウェア再送信制限を設定します。

undo short-retry threshold コマンドは、デフォルトに戻します。

RTS しきい値以下のフレームのハードウェア再送信制限を設定します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

AP ap 1 の小さいフレームのハードウェア再送信制限を 10 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] short-retry threshold 10

AP グループ apgroup 1 の QX-W 1020 モデルの AP で、小さいフレームのハードウェア再送信制限を 10 に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] short-retry threshold 10

関連コマンド

- **long-retry threshold**
- **protection-threshold**

1.1.58 smart-antenna

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

smart-antenna { disable | enable }

undo smart-antenna

デフォルト

Radio view では、無線は AP group’s radio view の設定を使用します。

AP group’s radio view では、スマートアンテナ機能が有効になります。

View

Radio view

AP group’s radio view

定義済みユーザロール

network-admin

説明

smart-antenna enable コマンドは、スマートアンテナ機能を有効にします。

smart-antenna disable コマンドは、スマートアンテナ機能を無効にします。

undo smart-antenna コマンドは、デフォルトに戻します。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax 無線にのみ適用できます。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#AP ap 1 のスマートアンテナを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] smart-antenna enable

#AP グループ apgroup 1 のスマートアンテナを有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] smart-antenna enable

1.1.59 smart-antenna policy

🕮 **メモ：**

このコマンドのサポートは、AP モデルによって異なります。

Syntax

smart-antenna policy { auto | high-availability | high-throughput }

undo smart-antenna policy

デフォルト

Radio view では、無線は AP group's radio view の設定を使用します。

AP group's radio view では、自動モードが使用されます。

View

Radio view

AP group’s radio view

定義済みユーザロール

network-admin

パラメータ

auto:自動モードを指定します。このモードを有効にすると、オーディオおよびビデオパケットには高可用性モードが使用され、その他のパケットには高スループットモードが使用されます。

high-availability:高可用性モードを指定します。このモードは、クライアントの帯域幅を保証し、安定した帯域幅を必要とする WLAN に適用できます。

high-throughput:高スループットモードを指定します。このモードは、できるだけ多くのアソシエーションを保証し、高いパフォーマンスを必要とする WLAN に適用できます。

説明

smart-antenna policy コマンドは、スマートアンテナモードを指定します。

undo smart-antenna policy コマンドは、デフォルトに戻します。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax 無線にのみ適用できます。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

スマートアンテナモードの設定は、スマートアンテナ機能を有効にした後でのみ有効になります。

Radio view の設定は、AP group’s radio view の設定よりも優先されます。

例

#AP ap 1 のスマートアンテナモードをハイアベイラビリティに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] smart-antenna policy high-availability

#AP グループ apgroup 1 のスマートアンテナモードを high-availability に設定します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] smart-antenna policy high-availability

1.1.60 stbc

Syntax

stbc { disable | enable }

undo stbc

デフォルト

Radio view では、無線は AP group's radio view の設定を使用します。

AP group's radio view では、STBC が有効になっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

stbc enable コマンドは、Space-Time Block Coding (STBC) を有効にします。

stbc disable コマンドは、STBC を無効にします。

undo stbc コマンドは、デフォルトに戻します。

このコマンドは、802.11n、802.11ac、802.11gac、802.11ax、および 802.11gax 無線にのみ適用できます。無線モードを 802.11a、802.11b、または 802.11g に変更すると、コマンドが無効になります。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#AP ap 1 の STBC を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

[AC-wlan-ap-ap1-radio-1] stbc enable

#AP グループ 1 の STBC を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] type dot11an

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] stbc enable

1.1.61 su-txbf

🕮 **メモ**:

このコマンドのサポートは、AP モデルによって異なります。

Syntax

su-txbf { disable | enable }

undo su-txbf

デフォルト

Radio view では、無線は AP group's radio view の設定を使用します。

AP group's radio view では、シングルユーザ TxBF は無効になっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

su-txbf enable コマンドは、シングルユーザ TxBF を有効にします。

su-txbf disable コマンドは、シングルユーザ TxBF を無効にします。

undo su-txbf コマンドは、デフォルトに戻します。

このコマンドは、802.11ac、802.11gac、802.11ax、および 802.11gax 無線にのみ適用できます。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドは無効になります。

シングルユーザ TxBF により、AP は目的の 1 つのクライアントへの信号を改善できます。シングルユーザ TxBF は、クライアントが広く普及し、ネットワーク品質が低く、深刻な信号減衰がある WLAN に適用できます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#AP ap 1 のシングルユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] su-txbf enable

#AP グループ apgroup 1 のシングルユーザ TxBF を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] su-txbf enable

関連コマンド

- **mu-txbf**

1.1.62 twt negotiate

🕮 **メモ**：

twt negotiate コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでサポートしています。

Syntax

twt negotiate { disable | enable }

undo twt negotiate

デフォルト

Radios view では、無線は AP group’s view の設定を使用します。

AP group’s radio view では、デフォルト設定は AP モデルによって異なります。

View

Radio view

AP group’s radio view

定義済みユーザロール

network-admin

説明

twt negotiate enable コマンドは、Target Wake Time (TWT) ネゴシエーションを有効にします。

twt negotiate disable コマンドは、TWT ネゴシエーションを無効にします。

undo twt negotiate コマンドは、デフォルトに戻します。

TWT ネゴシエーションを使用すると、クライアントと AP はサービス期間中にのみデータパケットを交換し、クライアントの休止状態をスケジュールして、クライアントの電力消費とワイヤレスリソースの競合を減らすことができます。

TWT ネゴシエーションを有効にすると、クライアントはサービス期間、TWT 間隔、最初のウェイク時間 (クライアントによって計算される) を伝えるネゴシエーション要求を AP に送信します。このような要求を受信すると、AP は応答を送信します。その後、クライアントは予定どおりに起動し、その AP からのトリガーフレームを待機します。トリガーフレームを受信すると、クライアントはサービス期間に入り、その AP とのデータパケットの交換を開始します。サービス期間が満了すると、データパケット交換が完了していない場合でも、クライアントは休止モードに入ります。

無線は、最大 8 つのクライアントに TWT サービスを提供できます。8 つのクライアントの TWT ネゴシエーション要求に応答した後、無線は他のクライアントからの要求を拒否します。

この機能は、802.11ax および 802.11gax 無線でのみ有効です。無線モードを非 802.11ax または非 802.11gax モードに変更すると、設定が削除されます。

Radio view の設定は、AP group’s radio view の設定よりも優先されます。

例

#AP ap 1 の無線 1 の TWT ネゴシエーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] twt negotiate enable

#AP グループ apgroup 2 の AP の無線 1 に対して TWT negotiation を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] twt negotiate enable

関連コマンド

- **type**

1.1.63 type

🕮 **メモ：**

QX-W1240 は 802.11be (draft)に対応しています。

Syntax

type { **dot11a** | **dot11abe** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11be** | **dot11eax** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gbe | dot11gn** }

undo type

デフォルト

QX-W1010 の Radio1、Radio2 の無線モードは、それぞれ dot11ac、dot11gn です。

QX-W1020、QX-W1030 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11ac、dot11ac、dot11gn です。

QX-W1110 の Radio1、Radio2 の無線モードは、それぞれ dot11ax、dot11gax です。

QX-W1120 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11ax、dot11ax、dot11gn です。

QX-W1130 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11ax、dot11ax、dot11gax です。

QX-W1210 の Radio1、Radio2 の無線モードは、それぞれ dot11abe、dot11gbe です。

QX-W1230 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11be、dot11abe、dot11gbe です。

QX-W1240 の Radio1、Radio2、Radio3 の無線モードは、それぞれ dot11be、dot11abe、dot11gbe です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a 無線モードを指定します。

dot11ac: 802.11ac 無線モードを指定します。

dot11an: 802.11n(5GHz)無線モードを指定します。

dot11ax: 802.11ax 無線モードを指定します。

dot11b: 802.11b 無線モードを指定します。

dot11be:802.11be(6GHz 帯) 無線モードを指定します。

dot11eax：802.11ax (6GHz 帯) 無線モードを指定します。

dot11g: 802.11g 無線モードを指定します。

dot11gac: 802.11gac 無線モードを指定します。

dot11gax: 802.11gax 無線モードを指定します。

dot11gbe：802.11be (2.4GHz 帯) 無線モードを指定します。

dot11gn: 802.11n (2.4 GHz) 無線モードを指定します。

🕮 **メモ：**

802.11ac を 2.4GHz で使用するモードを 802.11gac と定義します。
802.11ax を 2.4GHz で使用するモードを 802.11gax と定義します。
802.11be を 2.4GHz で使用するモードを 802.11gbe と定義します。

説明

type コマンドは、無線モードを指定します。

undo type コマンドは、デフォルトに戻します。

⚠ **注意：**

有効になっている無線のモードを変更すると、すべての接続されたクライアントが接続解除されます。

メモ：

- QX-W1100 シリーズは Raido3 で 802.11a、ac、an も指定できますが設定した場合 Raido3 が無効になります。
- QX-W1120 は Radio3 で 802.11gax を設定することができません。Radio 3 を 802.11a、ac、an のいずれかに設定することで、Radio 2 を 802.11gax に設定することができます。

AP group's radio view で無線モードを変更すると、無線モード関連コマンドのデフォルト設定が復元されます。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

AP **ap1** の無線 1 で、無線モードを 802.11n (5 GHz)に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11an

#AP グループ apgroup 1 の無線 1 の無線モードを 802.11n (5 GHz) に設定します。<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11an

1.1.64 ul-ofdma

メモ：

ul-ofdma コマンドは QX-W1100 シリーズおよび QX-W1200 シリーズでのみサポートしています。

Syntax

ul-ofdma { disable | enable }

undo ul-ofdma

デフォルト

Radio view では、AP は AP group’s radio view の設定を使用します。

AP group’s radio view では、アップリンク OFDMA は無効になっています。

View

Radio view

AP group’s radio view

定義済みユーザロール

network-admin

説明

ul-ofdma enable コマンドは、アップリンク OFDMA を有効にします。

ul-ofdma disable コマンドは、アップリンク OFDMA を無効にします。

undo ul-ofdma コマンドは、デフォルトに戻します。

このコマンドは、802.11ax および 802.11gax 無線でのみ有効です。無線モードを 802.11a/b/g/n/ac/gac に変更すると、設定が削除されます。

OFDMA は、小さなデータパケットが送信される高密度環境で有効にすると、次の利点を提供できます。

- 複数のユーザへの同時送信。
- 無線使用の改善。
- 伝送遅延の短縮。
- 競合バックオフの削減。

Radio view の設定は、APgroup's radio view の設定よりも優先されます。

例

#AP ap 1 の無線 1 のアップリンク OFDMA を無効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] type dot11ax

[AC-wlan-ap-ap1-radio-1] ul-ofdma disable

#AP グループ apgroup 1 の AP の無線 1 のアップリンク OFDMA を無効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1]ap-model QX-W1020

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] type dot11ax

[AC-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] ul-ofdma disable

関連コマンド

- **type dot11ax**

1.1.65 wlan in-band 6g-discovery

🕮 **メモ**：

wlan in-band 6g-discovery コマンドはソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

Syntax

wlan in-band 6g-discovery { enable | mode { fils | upr } }

undo wlan in-band 6g-discovery { enable | mode }

デフォルト

無効

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

enable : 6GHz の無線サービスの検出機能を有効にします。

mode fils : 6GHz の無線サービスの検出方法として **fils** モードを指定します。

mode upr : 6GHz の無線サービスの検出方法として **upr** モードを指定します。

説明

wlan in-band 6g-discovery コマンドは、6GHz の無線サービスの検出機能を有効にし、無線サービスの検出方法を設定します。

undo wlan in-band 6g-discovery コマンドはデフォルトに戻します。

この機能を有効にすると、6GHz 無線で有効になっている無線サービスの情報を、以下のいずれかのフレームを 6GHz 無線から送信することで検出できるようにします。

- **fils** モードでは、FILS(Fast Initial Link Setup）discovery フレームを使用して 6GHz の無線サービスを検出します。FILS discovery フレームは圧縮ビーコンフレームであり、SSID、BSSID、およびチャネルなどの重要な情報のみを含みます。この方法が構成されていると、AP の 6GHz 無線は 20 ミリ秒の間隔で FILS discovery フレームをブロードキャストします。無線サービスの検出方法を指定せずにこの機能を有効にした場合、**fils** モードが使用されます。
- **upr** モードでは、UPR(Unsolicited Probe Response)フレームを使用して 6GHz 無線サービスを検出します。UPR フレームはビーコンフレームと同じ詳細情報を含みます。この方法が構成されていると、AP の 6GHz 無線は 20 ミリ秒の間隔で UPR をブロードキャストします。

例

6GHz 帯無線サービス検出機能を有効にし、検出方法として **fils** を指定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] wlan in-bound 6g-discovery enable

[AC-wlan-global-configuration] wlan in-band 6g-discovery mode fils

1.1.66 wlan multiple-bssid enable

🕮 メモ：

wlan multiple-bssid enable コマンドはソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

Syntax

wlan multiple-bssid enable

undo wlan multiple-bssid

デフォルト

無効

View

Global configuration view

定義済みユーザロール

network-admin

説明

wlan multiple-bssid enable コマンドは、マルチ BSSID 機能を有効にします。

undo wlan multiple-bssid コマンドはデフォルトに戻します。

この設定は 6GHz 無線を使用するときに有効にします。

この機能を有効にすると、AP は 1 つのビーコンフレームまたはプローブ応答に複数の BSSID に関する情報を含めて送信します。

例

#マルチ BSSID 機能を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] wlan multiple-bssid enable

1.1.67 wlan out-band 6g-discovery

🕮 メモ：

wlan out-band 6g-discovery enable コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

wlan out-band 6g-discovery enable

undo wlan out-band 6g-discovery enable

デフォルト

有効

View

Global configuration view

定義済みユーザロール

network-admin

説明

wlan out-band 6g-discovery enable コマンドは、6GHz 帯無線サービス検出機能を有効にします。

undo wlan out-band 6g-discovery enable コマンドはデフォルトに戻します。

この設定は 6GHz 無線を使用するときに有効にします。

6GHz 帯無線サービス検出機能を有効にすると、AP の 6GHz 無線インタフェースで有効になっている BSSID の情報を、5GHz または 2.4GHz の無線から送信するパケット内に追加して送信します。

6GHz 無線に対応したクライアントは AP の 2.4GHz または 5GHz の無線から送信されたパケット内の BSSID の情報を読み取ることで、AP の 6GHz 無線を検出することができます。

この設定を使用する場合は、AP の Radio2(5GHz)、または、Radio3(2.4GHz)を有効にして、サービステンプレートを割り当てる必要があります。

例

#AP ap1 の radio2 にサービステンプレート radio2 を割り当て、 6GHz 帯無線サービス検出機能を有効にします。

<AC> system-view

[AC] wlan service-template radio2

[AC-wlan-st-radio2] ssid radio2

[AC-wlan-st-radio2] service-template enable

[AC-wlan-st-radio2] quit

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] radio enable

[AC-wlan-ap-ap1-radio-2] wlan service-template radio2

[AC-wlan-ap-ap1-radio-2] return

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] wlan out-bound 6g-discovery enable

1.1.68 wlan radio

Syntax

wlan radio { disable | enable }

undo wlan radio

デフォルト

radio view または AP group radio view で無線が有効になっていない場合、無線は無効になります。

View

System view

定義済みユーザロール

network-admin

説明

wlan radio enable コマンドは、すべての無線を有効にします。

wlan radio disable コマンドは、すべての無線を無効にします。

undo wlan radio コマンドは、デフォルトに戻します。

注意

この機能は、すべての手動 AP とオンライン自動 AP で有効になります。

---

wlan radio コマンドと **radio** コマンドの両方を実行すると、最新の設定が有効になります。

例

無線を有効にします。

<AC> system-view

[AC] wlan radio enable

目次

このセクションのページは **9-x-x** です。

2 章 WLAN 無線ロードバランス 2-1
2.1 WLAN 無線ロードバランス設定コマンド 2-1
2.1.1 wlan radio-load-balance overload-5g ssid-hide 2-1

2章 WLAN 無線ロードバランス

2.1 WLAN無線ロードバランス設定コマンド

2.1.1 wlan radio-load-balance overload-5g ssid-hide

Syntax

wlan radio-load-balance overload-5g ssid-hide { **disable** | **enable** [**session value** [**gap gap-value**]] }

undo wlan radio-load-balance overload-5g ssid-hide

デフォルト

AP view:AP グループ設定を継承します。

AP group's view:過負荷 5 G 無線隠し SSID 機能がオンになっています。

View

AP view

AP group's view

定義済みユーザロール

network-admin

パラメータ

session *value*:セッションしきい値。範囲は 1~120 で、デフォルト値は 5 です。

gap *gap-value*:セッションの差分しきい値。範囲は 1~24 で、デフォルトは 4 です。セッションの差は、現在の 5 G 無線のオンラインクライアントの数と、同じ AP 内の別の 5 G 無線のオンラインクライアントの数の差です。

説明

wlan radio-load-balance overload-5g ssid-hide enable コマンドは、過負荷 5 G 無線周波数非表示 SSID 機能をオンにするために使用します。

wlan radio-load-balance overload-5g ssid-hide disable コマンドは、過負荷 5 G 無線周波数非表示 SSID 機能をオフにするために使用します。

undo wlan radio-load-balance overload-5g ssid-hide コマンドを使用して、デフォルトの状態を復元します。

本機能をオンにした後、5 G 無線周波数上のオンラインクライアントの数がセッションしきい値に到達または超過し、かつ同じ AP 内の別の 5 G 無線周波数上のオンラインクライアントの数との差がセッションしきい値に到達または超過する場合、本無線周波数

は SSID を隠し、過負荷 5 G 無線周波数のアクセス数を低下させる。オンラインクライアントの数がセッションしきい値より少ない場合、またはセッションの差が差のしきい値に達していない場合、無線周波数は SSID を非表示にしなくなりました。

現在の環境でクライアントの数が多すぎる場合は、この機能を有効にすることをお勧めします。

この機能は、AP に複数の 5 GHz 無線がある場合にのみ有効です。

例

#オーバーロード 5 G 無線周波数非表示 SSID 機能をオンにし、セッションしきい値を 20 に設定し、セッション差分しきい値を 5 に設定します。(AP view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] wlan radio-load-balance overload-5g ssid-hide enable session 20 gap 5

#オーバーロード 5 G 無線周波数非表示 SSID 機能をオンにし、セッションしきい値を 20 に設定し、セッション差分しきい値を 5 に設定します。(AP group's view)

<Sysname> system-view

[Sysname] wlan ap-group group1

[Sysname-wlan-ap-group-group1] wlan radio-load-balance overload-5g ssid-hide enable session 20 gap 5

目次

このセクションのページは **9-x-x** です。

3 章 WLAN ロードバランス 3-1
3.1 WLAN ロードバランス設定コマンド 3-1
3.1.1 ap radio 3-1
3.1.2 description 3-2
3.1.3 display wlan load-balance group 3-2
3.1.4 display wlan load-balance status service-template 3-4
3.1.5 snmp-agent trap enable wlan load-balance 3-5
3.1.6 wlan load-balance access-denial 3-6
3.1.7 wlan load-balance enable 3-7
3.1.8 wlan load-balance group 3-7
3.1.9 wlan load-balance mode bandwidth 3-8
3.1.10 wlan load-balance mode session 3-9
3.1.11 wlan load-balance mode traffic 3-10
3.1.12 wlan load-balance rssi-threshold 3-11

3章 WLAN ロードバランス

3.1 WLANロードバランス設定コマンド

3.1.1 ap radio

Syntax

ap name *ap-name* **radio** *radio-id*

undo ap { name *ap-name* **[radio** *radio-id* **] | all }**

デフォルト

設定なし

View

Load balancing group view

定義済みユーザロール

network-admin

パラメータ

ap-name:AP を名前で指定します。1 から 64 文字の文字列で、大文字と小文字が区別されます。名前には、文字、数字、アンダースコア(_)、ドット（。）、左かっこ（[）、右括弧(])）、スラッシュ(/)、およびマイナス記号(-)を含めることができます。AP はすでに存在している必要があります。

radio-id:ID で無線を指定します。

all:すべての無線を指定します。

説明

ap radio を使用して、ロードバランシンググループに無線を追加します。

undo ap を使用して、ロードバランシンググループから 1 つまたはすべての無線を削除します。

無線を追加できるロードバランシンググループは 1 つだけです。

undo ap コマンドで無線を指定しない場合、コマンドは指定された AP 上のすべての無線をロードバランシンググループから削除します。

例

ロードバランシンググループ 10 に ap1 の radio2 を追加します。

<Sysname> system-view

[Sysname] wlan load-balance group 10

[Sysname-wlan-lb-group-10] ap name ap1 radio 2

3.1.2 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Load balancing group view

定義済みユーザロール

network-admin

パラメータ

text:ロードバランシンググループの説明を指定します。1 から 64 文字の文字列で、大文字と小文字が区別されます。

説明

description を使用して、ロードバランシンググループの説明を設定します。

undo description を使用して、デフォルトに戻します。

例

ロードバランシンググループの説明を marketing に設定します。

<Sysname> system-view

[Sysname] wlan load-balance group 10

[Sysname-wlan-lb-group10] description marketing

3.1.3 display wlan load-balance group

Syntax

display wlan load-balance group { *group-id* **| all }**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id:ロードバランシンググループを ID で指定します。この引数の値の範囲は 1 から 65535 です。

all:すべての負荷分散グループを指定します。

説明

負荷分散グループ情報を表示するには、**display wlan load-balance group** を使用します。

例

ロードバランシンググループ 1 のグループ情報を表示します。

<Sysname> display wlan load-balance group 1

```
               WLAN load balance group information
-------------------------------------------------------------------------------
Group ID             : 1
Description           :
Group members         : ap3-radio2,
                      ap2-radio1,
                      ap1-radio1,
-------------------------------------------------------------------------------
```

すべてのロードバランシンググループのグループ情報を表示します。

<Sysname> display wlan load-balance group all

```
               WLAN load balance group information
-------------------------------------------------------------------------------
Group ID             : 1
Description           :
Group members         : ap3-radio2,
                      ap2-radio1,
                      ap1-radio1,
-------------------------------------------------------------------------------
Group ID             : 2
Description           : marketing
Group members         : ap3-radio1,
-------------------------------------------------------------------------------
```

表 3-1 コマンド出力

フィールド	説明
Group members	ロードバランシンググループに存在する無線のリスト

3.1.4 display wlan load-balance status service-template

Syntax

display wlan load-balance status service-template *template-name* **client** *mac-address*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

template-name：サービステンプレート名を、大文字と小文字を区別しない 1～63 文字で指定します。

client *mac-address*：指定したクライアントを検出した無線に関する情報を表示します。mac-address 引数は、クライアントの MAC アドレスを表し、H-H-H 形式です。

説明

display wlan load-balance status service-template コマンドで、無線のロードバランシング情報を表示します。

例

#サービステンプレート st1 にバインドされた、MAC アドレス 702 d-2249-33 bf のクライアントを検出する無線のロードバランシング情報を表示します。

<Sysname> display wlan load-balance status service-template st1 client 702d-2249-33bf

```
Current load balancing mode (threshold/gap): session (2/1)
Load balancing group exist: No
Total radios: 4

APID/RID  Group ID  Session  Bandwidth(Mbps)  Traffic(%)  Balance(Y/N)
------------------------------------------------------------------------------
3/1       0         2        100              5           Y
1/2       0         10       50               10          N
4/1       0         2        10               1           Y
```

```
4/2        0          2          0                  0          Y
```

表 3-2 コマンド出力

フィールド	説明
Load-balance group exist	ロードバランシンググループが存在するかどうか:YesまたはNo。このフィールドは、現在のソフトウェアバージョンではサポートされていません。
APID/RID	AP IDまたは無線ID
Group ID	ロードバランシンググループID。0の値は、無線がロードバランシンググループに属していないことを示します。このフィールドは、現在のソフトウェアバージョンではサポートされていません。
Session	無線に関連付けられているクライアントの数
Bandwidth(Mbps)	無線の帯域幅
Traffic(%)	無線の最大帯域幅に対する無線のトラフィックの割合
Balance(Y/N)	ロードバランシングのステータス: • **Y**: 無線はロードバランスされています。 • **N**: 無線はロードバランスされていません。

3.1.5 snmp-agent trap enable wlan load-balance

Syntax

snmp-agent trap enable wlan load-balance

undo snmp-agent trap enable wlan load-balance

デフォルト

無効

View

system view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan load-balance コマンドで、WLAN ロードバランスの SNMP 通知を有効にします。

undo snmp-agent trap enable wlan load-balance コマンドで、WLAN ロードバランスの SNMP 通知を無効にします。

重大な WLAN ロードバランシングイベントを NMS に報告するには、WLAN ロードバランシングの SNMP 通知を有効にします。WLAN ロードバランシングイベント通知を正しく送信するには、デバイスで SNMP も設定する必要があります。SNMP 設定の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

例

#WLAN ロードバランシングの SNMP 通知を有効にする。

<Sysname> system-view

[Sysname] snmp-agent trap enable wlan load-balance

3.1.6 wlan load-balance access-denial

Syntax

wlan load-balance access-denial *access-denial*

undo wlan load-balance access-denial

デフォルト

10

View

system view

定義済みユーザロール

network-admin

パラメータ

access-denial：アソシエーション要求に対する拒否の最大数を 2 から 10 の範囲で指定します。

説明

wlan load-balance access-denial コマンドで、アソシエーション要求に対する拒否の最大数を設定します。

undo wlan load-balance access-denial コマンドで、デフォルトに戻ります。

AP がクライアントを拒否する回数がアソシエーション要求の拒否の最大数に達すると、AP はクライアントからアソシエーション要求を受け入れます。

例

#アソシエーション要求に対する拒否の最大数を 4 に設定する。

<Sysname> system-view

[Sysname] wlan load-balance access-denial 4

3.1.7 wlan load-balance enable

Syntax

wlan load-balance enable

undo wlan load-balance enable

デフォルト

無効

View

system view

定義済みユーザロール

network-admin

説明

wlan load-balance enable コマンドで、WLAN ロードバランスを有効にします。

undo wlan load-balance enable コマンドで、WLAN ロードバランスを無効にします。

例

#WLAN ロードバランシングを有効にする。

<Sysname> system-view

[Sysname] wlan load-balance enable

3.1.8 wlan load-balance group

Syntax

wlan load-balance group *group-id*

undo wlan load-balance group { *group-id* **| all }**

デフォルト

設定なし

View

system view

定義済みユーザロール

network-admin

パラメータ

group-id:ロードバランシンググループを ID で指定します。この引数の値の範囲は 1 から 65535 です。

all:すべての負荷分散グループを指定します。

説明

wlan load-balance group を使用してロードバランシンググループを作成し、そのビューを入力するか、既存のロードバランシンググループのビューを入力します。

undo wlan load-balance group を使用して、1 つまたはすべてのロードバランシンググループを削除します。

特定の AP 間でロードバランシングを実行するには、これらの AP の無線をロードバランシンググループに追加します。デバイスは、ロードバランシンググループに属さない無線ではロードバランシングを実行しません。

例

ロードバランシンググループ 10 を作成する。

<Sysname> system-view

[Sysname] wlan load-balance group 10

[Sysname-wlan-lb-group-10]

3.1.9 wlan load-balance mode bandwidth

Syntax

wlan load-balance mode bandwidth *value* **[gap** *gap-value* **]**

undo wlan load-balance mode

デフォルト

有効

定義済みユーザロール

network-admin

パラメータ

value： 帯域幅のしきい値を 1 から 500 Mbps の範囲で指定します。

gap *gap-value*： 帯域幅ギャップしきい値を 1～200 Mbps の範囲で指定します。デフォルトは 20 Mbps です。

説明

wlan load-balance mode bandwidth コマンドで、帯域幅モードのロードバランシングを設定します。

undo wlan load-balance mode コマンドで、デフォルトに戻します。

次の条件が満たされると、デバイスは帯域幅モードのロードバランシングを実行します。

- AP の帯域幅が帯域幅しきい値に達した。
- AP と最小の帯域幅を持つ AP 間の帯域幅ギャップが、しきい値に達した。

例

#負荷分散モードを bandwidth mode に設定し、bandwidth threshold と bandwidth gap threshold をそれぞれ 100 Mbps と 20 Mbps に設定する。

<Sysname> system-view

[Sysname] wlan load-balance mode bandwidth 100 gap 20

3.1.10 wlan load-balance mode session

Syntax

wlan load-balance mode session *value* [**gap** *gap-value*]

undo wlan load-balance mode

デフォルト

セッションモードロードバランシングが使用され、セッションしきい値は 20 です。

View

system view

定義済みユーザロール

network-admin

パラメータ

value： セッションしきい値を 1～120 の範囲で指定します。

gap *gap-value*： セッションギャップのしきい値を 1～12 の範囲で指定します。デフォルトのしきい値は 4 です。

説明

wlan load-balance mode session コマンドで、セッションモードのロードバランシングを設定します。

undo wlan load-balance mode コマンドで、デフォルトに戻ります。

次の条件が満たされると、AC はセッションモードのロードバランシングを実行します。

- AP に関連付けられているクライアントの数がセッションしきい値に達した。
- AP とクライアント数が最も少ない AP との間のセッションギャップは、セッションギャップしきい値に達した。

例

#ロードバランシングモードをセッションモードに設定し、セッションしきい値とセッションギャップしきい値をそれぞれ 7 と 5 に設定する。

<Sysname> system-view

[Sysname] wlan load-balance mode session 7 gap 5

3.1.11 wlan load-balance mode traffic

Syntax

wlan load-balance mode traffic *value* [**gap** *gap-value*]

undo wlan load-balance mode

デフォルト

有効

View

system view

定義済みユーザロール

network-admin

パラメータ

value： トラフィックと AP の最大帯域幅の比率でトラフィックしきい値を指定します。この引数の値の範囲は 1~80%です。

gap *gap-value*：AP のトラフィックギャップと最大帯域幅の比率のトラフィックギャップしきい値を指定します。この引数の値の範囲は 10～40%です。デフォルトのしきい値は 20%です。

説明

wlan load-balance mode traffic コマンドで、トラフィックモードのロードバランシングを設定します。

undo wlan load-balance mode コマンドで、デフォルトに戻ります。

次の条件が満たされた場合、AC はトラフィックモードロードバランシングを実行します。

- AP のトラフィックがトラフィックしきい値に達した。
- AP とトラフィックが最小の AP との間のトラフィックギャップは、トラフィックギャップしきい値に達した。

例

#ロードバランシングモードをトラフィックモードにし、トラフィックしきい値とトラフィックギャップしきい値をそれぞれ 25%と 20%に設定する。

<Sysname> system-view

[Sysname] wlan load-balance mode traffic 25 gap 20

3.1.12 wlan load-balance rssi-threshold

Syntax

wlan load-balance rssi-threshold rssi-threshold

undo wlan load-balance rssi-threshold

デフォルト

25

View

system view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold : RSSI しきい値を 5 から 100 の範囲で指定します。

説明

wlan load-balance rssi-threshold コマンドで、受信信号強度インジケータ (RSSI) のしきい値を設定します。

undo wlan load-balance rssi-threshold コマンドで、デフォルトに戻ります。

AP は、クライアントの RSSI がロードバランシングの RSSI しきい値よりも低い場合、クライアントが検出されないと判断します。1 つの AP だけがクライアントを検出できる場合、AP はクライアントの拒否の最大数を 1 に減らすことで、クライアントのアクセス確率を高めます。

例

#RSSI しきい値を 40 に設定する。

<Sysname> system-view

[Sysname] wlan load-balance rssi-threshold 40

目次

このセクションのページは **9-x-x** です。

4 章 WLAN 無線リソース計測 4-1
4.1 WLAN 無線リソース計測設定コマンド 4-1
4.1.1 display wlan measure-report 4-1
4.1.2 measure 4-6
4.1.3 measure-duration 4-7
4.1.4 measure-interval 4-9
4.1.5 resource-measure 4-10
4.1.6 rm-capability mode 4-11

4章 WLAN 無線リソース計測

4.1 WLAN無線リソース計測設定コマンド

4.1.1 display wlan measure-report

Syntax

display wlan measure-report ap *ap-name* **radio** *radio-id* [**client mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*:クライアントが関連付けられている AP を指定します。1~64 文字の文字列で、英字、数字、アンダースコア、 「.」 、[」 、 「]、 「/」 、 「-」 を使用でき、大文字と小文字が区別されます。

radio *radio-id*:AP の無線番号を指定します。値の範囲はアクセスポイントデバイスのモデルに依存します。デバイスの実際の状態に基づいてください。

client mac-address *mac-address*:クライアントの MAC アドレスを H-H-H 形式で指定します。client mac-address パラメータを指定しない場合は、すべてのクライアントの計測情報が表示されます。

説明

display wlan measure-report コマンドを使用して、クライアントの計測レポート情報を表示します。

例

#クライアントの計測レポート情報を表示します。

<Sysname> display wlan measure-report ap ap1 radio 2

```
Total number of clients: 1

Client MAC address                          : 0aef-e760-3587
Link measurement:
  Link margin                               : 2dBm
```

```
  RCPI                                  : -85 dBm
  RSNI                                  : 53 dBm
Noise histogram:
  Antenna ID                             : 3
  ANPI                                  : -56 dBm
  IPI0 to IPI10 density                    : 5 12 16 13 8 5 5 15 17 1 3
Spectrum measurement:
  Transmit power                         : 20 dBm
  BSS                                   : Detected
  OFDM preamble                          : Detected
  Radar                                 : Detected
  Unidentified signal                    : Undetected
  CCA busy fraction                      : 60
  RPI0 to RPI7 density                    : 3 7 11 19 15 23 15 7
Frame report entry:
  BSSID                                 : a072-2351-e253
  PHY type                              : fhss
  Average RCPI                           : -10 dBm
  Last RSNI                             : 2 dBm
  Last RCPI                             : -20 dBm
  Frames                                : 1
Dot11BSSAverageAccessDelay group:
  Average access delay                    : 32 ms
  BestEffort average access delay          : 1 ms
  Background average access delay          : 1 ms
  Video average access delay              : 1 ms
  Voice average access delay              : 1 ms
  Clients                               : 32
  Channel utilization rate                 : 11
Transmit stream:
  Traffic ID                            : 0
  Sent MSDUs                            : 60
  Discarded MSDUs                        : 5
  Failed MSDUs                          : 3
  MSDUs resent multiple times              : 3
  Lost QoS CF-Polls                      : 2
  Average queue delay                    : 2 ms
  Average transmit delay                  : 1 ms
  Bin0 range                            : 0 to 10 ms
  Bin0 to Bin5                           : 5 10 10 5 10 10
```

表 4-1 display wlan measure-report コマンドの表示情報の説明

フィールド	説明
Client MAC address	クライアントのMACアドレス
Link measurement	リンク計測情報
Link margin	受信したクライアントのメッセージ電力と最小許容電力の差である、クライアントリンクの冗長性の値
RCPI	クライアントがチャネル電力を受信
RSNI	クライアント受信信号対雑音比
Noise histogram	雑音ヒストグラム情報
Antenna ID	クライアントのアンテナ番号
ANPI	計測中のチャネルの平均雑音電力
IPI0 to IPI10 density	IPI 0~IPI10計測期間中の経過時間と全経過時間の割合 IPIn (n=0~10)は異なるIPI電力間隔を表します。 ● 0:IPI<=–92 dBm ● 1:–92 dBm<IPI<=–89 dBm ● 2:–89 dBm<IPI<=–86 dBm ● 3:–86 dBm<IPI<=–83 dBm ● 4:–83 dBm<IPI<=–80 dBm ● 5:–80 dBm<IPI<=–75 dBm ● 6:–75 dBm<IPI<=–70 dBm ● 7:–70 dBm<IPI<=–65 dBm ● 8:–65 dBm<IPI<=–60 dBm ● 9:–60 dBm<IPI<=–55 dBm ● 10:–55 dBm<IPI
Spectrum measurement	スペクトル管理計測情報
Transmit power	クライアントの送信電力
BSS	計測中にクライアントが他の802.11ネットワークメッセージを検出したかどうか
OFDM preamble	計測中にクライアントがOFDMプリアンブルを検出したかどうか
Radar	計測中にクライアントがレーダー信号を検出したかどうか
Unidentified signal	計測中にクライアントが非802.11ネットワーク、非OFDMネットワーク、非レーダーの未知の信号を検出したかどうか
CCA busy fraction	計測中のチャネルビジー時間が全計測時間に占める割合

フィールド	説明
RPI0 to RPI7 density	計測期間中のRPI 0~RPI 7の経過時間と全体の経過時間の割合 RPIn (n=0~7)は、異なるRPI電力間隔を表します。 ● 0:RPI<=-87 dBm ● 1:-87 dBm<RPI<=-82 dBm ● 2:-82 dBm<RPI<=-77 dBm ● 3:-77 dBm<RPI<=-72 dBm ● 4:-72 dBm<RPI<=-67 dBm ● 5:-67 dBm<RPI<=-62 dBm ● 6:-62 dBm<RPI<=-57 dBm ● 7:-57 dBm<RPI
Frame report entry	フレーム・レポート・テーブル・アイテム情報
BSSID	基本サービスセットID
PHY type	メディアタイプ: ● fhss ● dsss ● irbaseband ● oftm ● hrdsss ● erp
Average RCPI	平均受信チャネル電力
Last RSNI	最新の信号対雑音比
Last RCPI	最新の計測された受信チャネル電力
Frames	計測中に受信した同じMACアドレスとBSSIDからのデータフレームと管理フレームの数
Dot11Counters group	dot11カウント統計グループ
Sent fragments	クライアントが送信したフレームクリップの数
Sent multicast frames	クライアントが送信したマルチキャストフレームの数
Failed frames	クライアントがフレームの送信に失敗した回数
Received fragments	クライアントが受信したフレーム・フラグメントの数
Received multicast frames	クライアントが受信するマルチキャストフレームの数
FCS errors	クライアント・フレームシーケンス・チェックエラーの回数
Sent frames	クライアントが送信したフレームの数
Dot11MACStatistics group	dot11メディアアクセス制御統計グループ
Retries	クライアント再送信フレーム数
Multiple retries	クライアントが複数回再送したフレームの数
Duplicate frames	クライアントレプリケーションフレームの数
Successful RTS	クライアントRTS操作が成功した回数
Failed RTS	クライアントのRTS操作が失敗した回数

フィールド	説明
Failed ACK	クライアントACK操作が失敗した回数
Dot11QosCounters group for UP0~UP 7	dot11Qosカウント統計グループ
QoS sent fragments	QoSクライアントが送信するフレームクリップの数
QoS failure	QoSクライアントがフレーム送信に失敗した数
QoS retries	QoSクライアントが再送信するフレームの数
QoS multiple retries	QoSクライアントが再送信するマルチキャストフレームの数
QoS duplicate frames	QoSクライアントがレプリケートするフレームの数
QoS successful RTS	QoSクライアントのRTS操作が成功した回数
QoS failed RTS	QoSクライアントのRTS操作が失敗した回数
QoS failed ACK	QoSクライアントのACKが失敗した回数
QoS received fragments	QoSクライアントが受信するフレームフラグメントの数
QoS sent frames	QoSクライアントが送信するフレームの数
QoS discarded frames	QoSクライアントがドロップしたメッセージの数
QoS received MPDUs	QoSクライアントが受信したMPDUの数
QoS received retries	QoSクライアントが受信を再試行する回数
Dot11BSSAverageAccessDelay group	dot11BSS平均アクセス遅延統計グループ
Average access delay	AP平均アクセス遅延統計
BestEffort average access delay	ベスト・エフォートフロー平均アクセス遅延統計
Background average access delay	バックグラウンドストリーム平均アクセス遅延統計
Video average access delay	ビデオストリーム平均アクセス遅延統計
Voice average access delay	音声ストリーム平均アクセス遅延統計
Clients	クライアント数統計
Channel utilization rate	チャネル使用率統計
Transmit stream	伝送ストリーム計測情報
Traffic ID	トランスポートストリームID
Sent MSDUs	クライアントが正常に送信したMSDUの数
Discarded MSDUs	クライアントがドロップしたMSDUの数
Failed MSDUs	クライアントが送信に失敗したMSDUの数
MSDUs resent multiple times	クライアントが再送信したMSDUの数
Lost QoS CF-Polls	クライアントが送信したQoS CF-POLLフレームの損失数
Average queue delay	ミリ秒の平均キュー待ち時間
Average transmit delay	ミリ秒の平均送信待ち時間
Bin0 range	MSDUの送信に成功した平均遅延ヒストグラムの最初のセグメントの遅延範囲をミリ秒で示します。

フィールド	説明
Bin0 to Bin5	平均遅延ヒストグラムにおける送信成功MSDU数の分布 Binx (x=0~5)は、さまざまな平均遅延範囲を表します。 • bin 0:Delay<10 ms • bin 1:10 ms<=Delay<20 ms • bin 2:20 ms<=Delay<40 ms • Bin 3:40 ms<=Delay<80 ms • Bin 4:80 ms<=Delay<160 ms • Bin 5:160 ms<=Delay

4.1.2 measure

Syntax

measure { **all** | **link** | **neighbor** | **radio** | **spectrum** | **tpc** } { **disable** | **enable** }

undo measure

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、計測機能がオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

all:すべての計測

link:リンク計測は、リンク計測要求フレームに対する RCPI, RSNI,リンク冗長性などの情報を計測する。

neighbor:ネイバー計測:ネイバーAP のチャネル番号、BSSID などの情報を計測します。

radio:チャネル負荷計測、ノイズ分布計測、Beacon 計測、Frame 計測、STA 統計計測、位置情報計測、およびトランスポートストリーム計測を含む無線周波数計測。

spectrum:Basic 計測、CCA 計測、RPI 計測などのスペクトル計測。

tpc:送信電力制御計測、クライアントのリンク冗長性と送信電力を計測する。

説明

measure enable コマンドを使用して、計測機能をオンにします。

measure disable コマンドは、計測機能をオフにします。

undo measure コマンドを使用して、デフォルトの状態を復元します。

link、neighbor、radio 計測は、無線リソース計測がオンになっている場合にのみ有効になります。

spectrum および tpc 計測機能は、スペクトル管理機能がオンになっている場合にのみ有効です。スペクトル管理機能の構成の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*9 無線管理*”の”*8 章 スペクトル管理の設定*”を参照してください。

spectrum および tpc 計測機能は、5 GHz 無線でのみサポートされます。

例

#ネイバー計測をオンにします。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] measure neighbor enable

#ネイバー計測をオンにします。(AP group’s radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] measure neighbor enable

関連コマンド

- **measure-duration**
- **measure-interval**
- **resource-measure**
- **spectrum-management**

4.1.3 measure-duration

Syntax

measure-duration *time*

undo measure-duration

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、計測期間は 500 TU です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

time:TU (Time Unit、1 TU=1024 マイクロ秒)単位で 1~10000 の範囲の時間を計測します。

説明

measure-duration コマンドを使用して、計測期間を設定します。

undo measure-duration コマンドを使用して、デフォルトの状態を復元します。

計測機能をオンにすると、 AP からクライアントへ送信される計測要求メッセージに配置された計測継続時間が持ち越される。

例

#計測期間を 512 TU に設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] measure-duration 512

#計測期間を 512 TU に設定します。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] measure-duration 512

関連コマンド

- **measure**
- **measure-interval**

4.1.4 measure-interval

Syntax

measure-interval *interval*

undo measure-interval

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、30 秒の間隔で計測要求を送信します。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

interval:計測要求を送信する間隔。範囲は 10~60 で、単位は秒です。

説明

measure-interval コマンドを使用して、計測要求を送信する間隔を設定します。

undo measure-interval コマンドを使用して、デフォルトの状態を復元します。

計測機能がオンになると、AP は設定された間隔で計測要求メッセージをクライアントに送信します。

例

#計測リクエストの送信間隔を 35 秒に設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] measure-interval 35

#計測リクエストの送信間隔を 35 秒に設定します。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] measure-interval 35

関連コマンド

- **measure**
- **measure-duration**

4.1.5 resource-measure

Syntax

resource-measure { **disable** | **enable** }

undo resource-measure

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、無線周波数リソース計測機能がオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

resource-measure enable コマンドを使用して、無線周波数リソース計測機能を有効にします。

resource-measure disable コマンドを使用して、無線周波数リソース計測機能をオフにします。

undo resource-measure コマンドを使用して、デフォルトの状態を復元します。

RF 資源計測機能をオンにした後:

- AP が送信する Beacon、Probe Response、Association Response、Reassociation Response の各フレームでは、 [Capability Set] フィールドの Radio Measurement ビットが設定され、AP がサポートする RF リソース計測情報をクライアントに送信し、AP が RF リソース計測をサポートしていること、およびサポートされている計測タイプを通知します。
- AP は、Measurement Pilot フレームを定期的に送信することで、クライアントが AP をより迅速にスキャンできるように支援します。Measurement Pilot メッセージは、Beacon フレームよりも高い頻度で送信されるが、Beacon フレームよりも少ない情報を運ぶ軽量な Beacon フレームと見なすことができる。

例

#無線周波数リソース計測を有効にします。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 2

[Sysname-wlan-ap-ap1-radio-2] resource-measure enable

#無線周波数リソース計測を有効にします。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] resource-measure enable

4.1.6 rm-capability mode

Syntax

rm-capability mode { **all** | **none** | **partial** }

undo rm-capability mode

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、クライアント無線周波数計測機能セットはチェックされません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

all:完全一致パターン。クライアントの無線周波数計測能力セットが AP の能力セットと完全に一致するまで、クライアントはオンラインになりません。そうでない場合、クライアントはオンラインになりません。

none:モードをチェックしません。つまり、クライアントの RF 計測能力セットをチェックしません。

partial:部分一致パターン。クライアントの無線周波数計測機能セットがデバイスの機能セットと一致する場合、クライアントはオンラインになります。一致しない場合、クライアントはオンラインになりません。

説明

rm-capability mode コマンドを使用して、クライアント無線周波数計測能力セットの検査モードを設定します。

undo rm-capability mode コマンドを使用して、デフォルトの状態を復元します。

RF 資源計測機能がオンになっている場合にのみ、RF 計測能力セットチェック機能が有効になります。

例

#クライアント無線周波数計測能力セットのチェックパターンを部分一致パターンに設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 2

[Sysname-wlan-ap-ap1-radio-2] resource-measure enable

[Sysname-wlan-ap-ap1-radio-2] rm-capability mode partial

#クライアント無線周波数計測能力セットのチェックパターンを部分一致パターンに設定します。(AP group’s radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] rm-capability mode partial

関連コマンド

- **resource-measure**

目次

このセクションのページは **9-x-x** です。

5 章 WLAN RRM 5-1
5.1 WLAN RRM 設定コマンド 5-1
5.1.1 adjacency-factor 5-1
5.1.2 ap name 5-2
5.1.3 calibrate-bandwidth self-decisive 5-3
5.1.4 calibrate-channel mode 5-5
5.1.5 calibrate-channel monitoring time-range 5-6
5.1.6 calibrate-channel pronto 5-8
5.1.7 calibrate-channel self-decisive 5-9
5.1.8 calibrate-channel channel-set-optimization 5-11
5.1.9 calibrate-channel channel-set-optimization neighbor-threshold 5-13
5.1.10 calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent5-14
5.1.11 calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set 5-16
5.1.12 calibrate-channel 2.4g channel-set-optimization enable 5-17
5.1.13 calibrate-channel 2.4g channel-set-optimization neighbor-threshold 5-19
5.1.14 calibrate-channel 2.4 g channel-set-optimization neighbor-unmanaged-threshold percent 5-20
5.1.15 calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set 5-21
5.1.16 calibrate-power 2.4g max 5-23
5.1.17 calibrate-power 2.4g min 5-24
5.1.18 calibrate-power 2.4g coverage rssi-threshold 5-25
5.1.19 calibrate-power 2.4g coverage weak-signal-client ratio 5-26
5.1.20 calibrate-power 2.4g coverage weak-signal-client threshold 5-27
5.1.21 calibrate-power 2.4g coverage weak-signal-packet ratio 5-28
5.1.22 calibrate-power 2.4g coverage weak-signal-packet threshold 5-30
5.1.23 calibrate-power 5g max 5-31
5.1.24 calibrate-power 5g min 5-32
5.1.25 calibrate-power 5g coverage rssi-threshold 5-33
5.1.26 calibrate-power 5g coverage weak-signal-client ratio 5-34
5.1.27 calibrate-power 5g coverage weak-signal-client threshold 5-35
5.1.28 calibrate-power 5g coverage weak-signal-packet ratio 5-36
5.1.29 calibrate-power 5g coverage weak-signal-packet threshold 5-38

5.1.30 calibrate-power 6g max 5-39
5.1.31 calibrate-power 6g min 5-40
5.1.32 calibrate-power 6g coverage rssi-threshold 5-41
5.1.33 calibrate-power 6g coverage weak-signal-client ratio 5-42
5.1.34 calibrate-power 6g coverage weak-signal-client threshold 5-43
5.1.35 calibrate-power 6g coverage weak-signal-packet ratio 5-44
5.1.36 calibrate-power 6g coverage weak-signal-packet threshold 5-46
5.1.37 calibrate-power coverage enable 5-47
5.1.38 calibrate-power min 5-49
5.1.39 calibrate-power mode 5-50
5.1.40 calibrate-power self-decisive 5-52
5.1.41 calibrate-power threshold 5-54
5.1.42 channel holddown-time 5-55
5.1.43 crc-error-threshold 5-56
5.1.44 description 5-57
5.1.45 display wlan rrm baseline 5-58
5.1.46 display wlan rrm baseline apply-history 5-60
5.1.47 display wlan rrm-calibration-group 5-62
5.1.48 display wlan rrm high-density filter history 5-64
5.1.49 display wlan rrm-history ap 5-65
5.1.50 display wlan rrm-status ap 5-67
5.1.51 interference-threshold 5-70
5.1.52 power holddown-time 5-71
5.1.53 rrm 5-72
5.1.54 scan-only 5-72
5.1.55 snmp-agent trap enable wlan rrm 5-74
5.1.56 tolerance-level 5-74
5.1.57 wlan calibrate-channel pronto ap all 5-76
5.1.58 wlan calibrate-power pronto ap all 5-77
5.1.59 wlan rrm baseline apply 5-78
5.1.60 wlan rrm baseline remove 5-78
5.1.61 wlan rrm baseline save 5-79
5.1.62 wlan rrm calibration-bandwidth interval 5-80
5.1.63 wlan rrm calibration-channel interval 5-81
5.1.64 wlan rrm calibration-power interval 5-82
5.1.65 wlan rrm-calibration-group 5-83
5.1.66 wlan rrm high-density filter 5-84

5章 WLAN RRM

5.1 WLAN RRM設定コマンド

5.1.1 adjacency-factor

Syntax

adjacency-factor *neighbor*

undo adjacency-factor

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :グローバル構成を継承します。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

パラメータ

neighbor **:** ネイバー係数。範囲は 1~16 です。

説明

ネイバーファクタを設定するには、**adjacency-factor** コマンドを使用します。

undo adjacency-factor コマンドを使用して、デフォルトの状態を復元します。

隣接係数は、電力比較閾値としても、電力比較の際に電力値を選択して電力調整閾値と比較するためにも使用される。

- 電力比較しきい値:Radio 情報を検出した他の Radio の数が電力比較しきい値に達すると、 AC は電力比較を行い、 Radio の電力を調整するかどうかを判断する。そうでない場合、Radio の送信電力は、最大送信電力に調整される。ネイバー係数が 3 である場合、AC は、Radio 情報が検出された他の Radio の数が 3 に達するまで電力比較を行わない。
- 電力比較のための電力値の選択:電力比較の場合、AC は、他の Radio によって検出されたこの Radio 電力値を大きい順にソートした後、隣接因子と同じ順位の電力値を選択し、すなわち、隣接因子が 3 であれば、3 位の電力値を選択して電力調整閾値と比較する。

RRM view の下の構成は、AP group's RRM view の下の構成よりも優先され、AP group's RRM view の下の構成は、グローバルビューの下の構成よりも優先されます。

例

#ネイバー係数を 7 に設定します。(RRM view)

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] adjacency-factor 7

#ネイバー係数を 7 に設定します。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] adjacency-factor 7

5.1.2 ap name

Syntax

ap name *ap-name* **radio** *radio-id*

undo ap { **name** *ap-name* [**radio** *radio-id*] | **all** }

デフォルト

RRM は、調整グループ内に AP が存在しない Radio を保持します。

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

name *ap-name*:RRM に参加すると、調整グループの AP 名が 1~64 文字の文字列で保持されます。この文字列には、英字、数字、アンダースコア、 「.」 、[」 、 「]、 「/」 、 「-」 を含めることができ、大文字と小文字が区別されます。

radio *radio-id*:AP の無線周波数を RRM ホールドダウン調整グループに結合します。ここで、radio-id は無線周波数番号です。このパラメータが指定されていない場合、RRM ホールドダウン調整グループで指定された AP のすべての無線周波数が削除されます。

all:RRM 保留調整グループ内のすべての無線周波数を削除します。

説明

ap name コマンドは、指定された Radio を RRM 保持調整グループに追加するために使用します。

undo ap name は、RRM 保持調整グループから Radio を削除するために使用されます。

RRM キープアライブ調整グループに参加する Radio はすでに存在する必要があります。

Radio は 1 つの RRM ホールドアップグループにのみ参加できます。Radio を新しい RRM ホールドアップグループに参加させると、元の RRM ホールドアップグループは Radio を削除します。

例

#ID 10 の RRM 保持調整グループに ap 1 の Radio 2 を追加します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] ap name ap1 radio 2

5.1.3 calibrate-bandwidth self-decisive

Syntax

RRM view/AP group's RRM view:

calibrate-bandwidth self-decisive { **disable** | **enable** }

undo calibrate-bandwidth self-decisive

Global configuration view:

calibrate-bandwidth self-decisive enable { **5g** | **6g** | **all** }

undo calibrate-bandwidth self-decisive enable { **5g** | **6g** | **all** }

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :グローバル構成を継承します。

Global configuration view:自動帯域幅調整がオフになっています。

View

RRM view

AP group's RRM view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

5g:すべての AP の 5 GHz 帯域無線の自動帯域幅調整機能のオン/オフを切り替えます。

6g: すべての AP の 6 GHz 帯域無線の自動帯域幅調整機能のオン/オフを切り替えます。

all:すべての AP の 5 GHz および 6GHz 帯域無線の自動チャネル調整機能をオンまたはオフにします。

🕮 **メモ：**

- **5g**、**6g**、**all** パラメータはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。
- ソフトウェアバージョン 9.4.05 のソフトウェアではパラメータの指定はできません。5GHz 帯域無線のみの自動帯域幅調整機能のオン/オフを切り替えます。

説明

calibrate-bandwidth self-decisive enable コマンドを使用して、自動帯域幅調整をオンにします。

calibrate-bandwidth self-decisive disable コマンドは、自動帯域幅調整をオフにします。

undo calibrate-bandwidth self-decisive コマンドを使用して、デフォルトの状態を復元します。

RF のネイバーRadio の数が多すぎる場合は、干渉を減らすために帯域幅を減らす必要があります。RF のネイバーRadio の数が少ない場合は、データ転送レートを上げるために帯域幅を増やす必要があります。帯域幅の増加または減少は、隣接するチャネルを結合または分割することによって行われる。

自動帯域幅調整をオンにすると、AC は自動帯域幅調整サイクルが完了するたびに帯域幅調整プロセスを開始します。

このコマンドは、5 GHz 帯無線でのみ有効です。

例

#自動帯域幅調整をオンにします。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-bandwidth self-decisive enable

#自動帯域幅調整をオンにします。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-bandwidth self-decisive enable

#すべての AP の 5 GHz 帯域無線の自動帯域幅調整機能を有効にします。(Global configuration view)

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-bandwidth self-decisive enable

5.1.4 calibrate-channel mode

Syntax

calibrate-channel mode { **periodic** | **scheduled** }

undo calibrate-channel mode

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :自動チャネル調整モードは定期的に調整されます。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

パラメータ

periodic:定期的に調整する。

scheduled:タイミング調整。

説明

calibrate-channel mode コマンドを使用して、自動チャネル調整モードを設定します。

undo calibrate-channel mode コマンドを使用して、デフォルトの状態を復元します。

周期性調整モードでは、 AC はユーザが設定した調整周期でチャネル品質の検出を繰り返し、検出結果からチャネル調整の要否を評価する。

タイミング調整モードでは、装置は指定された時間帯にチャネル品質情報を収集し、その後チャネル品質の評価を行い、チャネルを調整するかどうかを決定する。

例

#自動チャネル調整モードをタイミング調整用に設定します。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel mode scheduled

#自動チャネル調整モードをタイミング調整用に設定します。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel self-decisive enble

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel mode scheduled

関連コマンド

- **calibrate-channel monitoring time-range**
- **calibrate-channel pronto**
- **wlan rrm calibration-channel interval**

5.1.5 calibrate-channel monitoring time-range

Syntax

calibrate-channel monitoring time-range *time-range-name*

undo calibrate-channel monitoring time-range

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :無線周波数環境情報を収集するための期間が指定されていません。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

パラメータ

time-range-name:期間の名前を 1~32 文字の文字列で指定します。大文字と小文字は区別されず、a~z または A~Z で始まる必要があります。混乱を避けるため、期間の名前に英語の all を使用することはできません。

説明

calibrate-channel monitoring time-range コマンドを使用して、チャネル品質検出機能の期間を指定します。

undo calibrate-channel monitoring time-range コマンドは、チャネル品質検出機能に指定された期間をキャンセルするために使用します。

チャネル品質検出機能に時間帯を指定した後、AC は指定した時間帯内にチャネル品質検出タスクを実行し、かつデータを収集してチャネル報告と近隣報告を生成し、チャネル品質評価に根拠を提供する。

例

#チャネル品質検出機能の期間を time1 で指定します。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel monitoring time-range time1

#チャネル品質検出機能の期間を time1 で指定します。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel monitoring time-range time1

関連コマンド

- **time-range**

5.1.6 calibrate-channel pronto

Syntax

calibrate-channel pronto

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

説明

チャネルの自動調整を実行するには、**calibrate-channel pronto** コマンドを使用します。

このコマンドは、タイミング自動チャネル調整に使用されます。

例

#チャネルの自動調整を 1 回実行します。(RRM view)

<AC> system-view

[AC] scheduler job calibration1

[AC-job-calibration1] command 1 system-view

[AC-job-calibration1] command 2 wlan ap ap1

[AC-job-calibration1] command 3 radio 1

[AC-job-calibration1] command 4 rrm

[AC-job-calibration1] command 5 calibrate-channel pronto

#チャネルの自動調整を 1 回実行します。(AP group's RRM view)

<AC> system-view

[AC] scheduler job calibration2

[AC-job-calibration2] command 1 system-view

[AC-job-calibration2] command 2 wlan ap-group g1

[AC-job-calibration2] command 3 ap-model QX-W1020

[AC-job-calibration2] command 4 radio 1

[AC-job-calibration2] command 5 rrm

[AC-job-calibration2] command 6 calibrate-channel pronto

5.1.7 calibrate-channel self-decisive

Syntax

RRM view/ AP group's RRM view :

calibrate-channel self-decisive { **disable** | **enable** }

undo calibrate-channel self-decisive

Global configuration view:

calibrate-channel self-decisive enable { **2.4g** | **5g** | **6g** | **all** }

undo calibrate-channel self-decisive { **2.4g** | **5g** | **6g** | **all** }

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :グローバル構成を継承します。

Global configuration view:自動チャネル調整がオフになっています。

View

RRM view

AP group's RRM view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

2.4g:すべての AP の 2.4 GHz 帯域無線の自動チャネル調整機能のオン/オフを切り替えます。

5g:すべての AP の 5 GHz 帯域無線の自動チャネル調整機能のオン/オフを切り替えます。

6g: すべての AP の 6 GHz 帯域無線の自動チャネル調整機能のオン/オフを切り替えます。

🕮 **メモ：**

6g パラメータはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

---

all: ソフトウェアバージョン 9.4.05 のソフトウェアではすべての AP の 2.4 GHz および 5 GHz 帯域無線の自動チャネル調整機能をオンまたはオフにします。ソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでは、すべての AP の 2.4 GHz、5 GHz、および 6GHz 帯域無線の自動チャネル調整機能をオンまたはオフにします。

説明

calibrate-channel self-decisive enable コマンドは、自動チャネル調整をオンにするために使用します。

calibrate-channel self-decisive disable コマンドを使用して、自動チャネル調整をオフにします。

undo calibrate-channel self-decisive コマンドを使用して、デフォルトの状態を復元します。

自動チャネル調整をオンにすると、AC は自動チャネル調整モードに従ってチャネルの検出、評価、および調整を実行します。

例

#自動チャネル調整をオンにします。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable

#自動チャネル調整をオンにします。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-channel self-decisive enable

#すべての AP の 2.4 GHz および 5 GHz 帯域無線の自動チャネル調整機能を有効にします。(Global configuration view)

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-channel self-decisive enable all

関連コマンド

- **calibrate-channel mode**

5.1.8 calibrate-channel channel-set-optimization

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel channel-set-optimization { **disable** | **enable** }

undo calibrate-channel channel-set-optimization

デフォルト

RRM view では、AP group RRM view の設定が使用されます。

AP group RRM view では、Global configuration view の設定が使用されます。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

説明

calibrate-channel channel-set-optimization enable コマンドは 2.4 GHz 無線のチャネル最適化を有効にします。

calibrate-channel channel-set-optimization disable コマンドは 2.4 GHz 無線のチャネル最適化を無効にします。

undo calibrate-channel channel-set-optimization コマンドはデフォルトに戻します。

異なるベンダの AP が混在した環境では、これらの AP を統一した方法で管理できず、異なるチャネルグループを使用する可能性があるため、2.4 GHz 無線に対して重大な干渉が発生する可能性があります。これは、ユーザーエクスペリエンスに大きな影響を与えます。

この機能を使用すると、AC は、auto DFS でサードパーティ製 AP の近隣無線で最も使用されるチャネルグループを採用できます。この操作により、異なるベンダの AP 間のチャネル間干渉を最大限に減らすことができます。

装置は、(1、6、11)、(1、7、13)、(2、7、12)、(3、8、13)、(4、9、14)のチャネルグループの検出をサポートしています。

周辺の無線には、次のタイプがあります。

- **Managed neighbor**– 同じ AC で管理されている AP 無線を検出した場合
- **Unmanaged neighbor**– 別の AC で管理されている AP 無線を検出した場合

この機能を有効にすると、次の条件がすべて満たされた場合、装置は自動 DFS 中に 2.4 GHz 無線のチャネル最適化を実行します。

- 周辺の合計数が設定されたしきい値に達するか、それを超えた場合
- 管理対象外の周辺の比率（管理対象外の周辺/周辺の合計）が設定されたしきい値に達した場合か、それを超えた場合
- 単一のチャネルグループ（管理対象外の周辺/周辺の合計）の管理対象外の周辺の比率が設定されたしきい値に達した場合か、それを超えた場合

このコマンドは、2.4 GHz 無線でのみ有効です。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

AP ap1 の 2.4 GHz 無線のチャネル最適化を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] rrm

[AC-wlan-ap-ap1-radio-2-rrm] calibrate-channel-set-optimization enable

AP グループ group 1 の QX-W1110 で 2.4 GHz 無線のチャネル最適化を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] radio 2

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2-rrm] calibrate-channel channel-set-optimization enable

関連コマンド

- **calibrate-power 2.4g channel-set-optimization enable**
- **calibrate-channel 2.4g channel-set-optimization neighbor-threshold**
- **calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent**
- **calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set**
- **calibrate-channel channel-set-optimization neighbor-threshold**

- **calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent**
- **calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set**

5.1.9 calibrate-channel channel-set-optimization neighbor-threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel channel-set-optimization neighbor-threshold *count*

undo calibrate-channel channel -set-optimization neighbor-threshold

デフォルト

RRM view では、AP group RRM view の設定が使用されます。

AP group RRM view では、Global configuration view の設定が使用されます。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

count：近隣数のしきい値を 1～1000 の範囲で設定します。

説明

calibrate-channel channel-set-optimization neighbor-threshold コマンドは周辺数のしきい値を設定します。

undo calibrate-channel channel-set-optimization neighbor-threshold コマンドはデフォルトに戻します。

このコマンドは、2.4 GHz 無線でのみ有効です。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

AP ap1 の周辺の数のしきい値を 11 に設定します。

<AC> system-view

[AC] wlan ap ap 1 model QX-W1110

[AC-wlan-ap-ap 1] radio 2

[AC-wlan-ap-ap 1-radio-2] rrm

[AC -wlan-ap-ap 1-radio-2-rrm] calibrate-channel-set-optimization neighbor-threshold 11

#AP グループ group 1 の QX-W1110 で、周辺の数のしきい値を 11 に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] radio 2

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-threshold 11

関連コマンド

- **calibrate-power 2.4g channel-set-optimization enable**
- **`calibrate-channel channel-set-optimization`**

5.1.10 calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent

🕮 **メモ**:

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent *percent*

undo calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent

デフォルト

RRM view では、AP group RRM view の設定が使用されます。

AP group RRM view では、Global configuration view の設定が使用されます。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent: 管理対象外の周辺の比率のしきい値を 1～100 の範囲で設定します。

説明

calibrate-channel channel-set-optimization neighbor-unmanaged-threshold コマンドは管理対象外の周辺の比率のしきい値を設定します。

undo calibrate-channel channel-set-optimization neighbor-unmanaged-threshold コマンドはデフォルトに戻します。

このコマンドは、2.4 GHz 無線でのみ有効です。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

AP ap 1 の管理対象外の周辺の比率しきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] rrm

[AC-wlan-ap-ap1-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent 20

AP グループ group1 の QX-W1110 で、管理対象外の周辺の比率のしきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] radio 2

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent 20

5.1.11 calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel- set-optimization neighbor-unmanaged-threshold percent-per-set *percent*

undo calibrate-channel-set-optimization neighbor-unmanaged-threshold percent-per-set

デフォルト

RRM view では、AP group RRM view の設定が使用されます。

AP group RRM view の RRM view では、Global configuration view の設定が使用されます。

View

RRM view

AP group RRM view

定義済みユーザロール

network-admin

パラメータ

percent: 管理対象外の周辺の比率のしきい値を 1～100 の範囲で設定します。

説明

calibrate-channel- set-optimization neighbor-unmanaged-threshold percent-per-set コマンドは単一のチャネルグループの管理対象外の近隣比率しきい値を設定します。

undo calibrate-channel- set-optimization neighbor-unmanaged-threshold percent-per-set コマンドはデフォルトに戻します。

このコマンドは、2.4 GHz 無線でのみ有効です。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

AP ap1 の単一のチャネルグループの管理対象外の近隣比率しきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 2

[AC-wlan-ap-ap1-radio-2] rrm

[AC-wlan-ap-ap1-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set 20

#AP グループ group 1 の QX-W1110 で、単一のチャネルグループの管理対象外の近隣比率しきい値を 20%に設定します。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1110

[AC-wlan-ap-group-group1-ap-model-QX-W1110] radio 2

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1110-radio-2-rrm] calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent 20

関連コマンド

- **calibrate-channel 2.4g channel-set-optimization enable**
- **calibrate-channel channel-set-optimization**

5.1.12 calibrate-channel 2.4g channel-set-optimization enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel 2.4g channel-set-optimization enable

undo calibrate-channel 2.4g channel-set-optimization enable

デフォルト

有効

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

*percent:*管理対象外の周辺の比率のしきい値を 1～100 の範囲で設定します。

説明

calibrate-channel 2.4g channel-set-optimization enable コマンドは 2.4 GHz 無線のチャネル最適化を有効にします。

undo calibrate-channel 2.4g channel-set-optimization enable コマンドは 2.4 GHz 無線のチャネル最適化を無効にします。

異なるベンダの AP が混在した環境では、これらの AP を統一した方法で管理できず、異なるチャネルグループを使用する可能性があるため、2.4 GHz 無線に対して重大な干渉が発生する可能性があります。これは、ユーザーエクスペリエンスに大きな影響を与えます。

この機能により、AC は、サードパーティ製 AP の周辺の無線で最も使用されるチャネルグループを自動 DFS で採用できます。この操作により、異なるベンダの AP 間のチャネル間干渉を最大限に減らすことができます。

装置は、(1、6、11)、(1、7、13)、(2、7、12)、(3、8、13)、(4、9、14)のチャネルグループの検出をサポートしています。

周辺の無線には、次のタイプがあります。

- **Managed neighbor**– 同じ AC で管理されている AP 無線を検出した場合
- **Unmanaged neighbor**– 別の AC で管理されている AP 無線を検出した場合

この機能を有効にすると、次の条件がすべて満たされた場合、装置は自動 DFS 中に 2.4 GHz 無線のチャネル最適化を実行します。

- 周辺の合計数が設定されたしきい値に達するか、それを超えた場合
- 管理対象外の周辺の比率（管理対象外の周辺/周辺の合計）が設定されたしきい値に達した場合か、それを超えた場合
- 単一のチャネルグループ（管理対象外の周辺/周辺の合計）の管理対象外の周辺の比率が設定されたしきい値に達した場合か、それを超えた場合

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

2.4 GHz 無線のチャネル最適化を無効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] undo calibrate-channel 2.4g channel-set-optimization enable

関連コマンド

- **calibrate-channel 2.4g channel-set-optimization neighbor-threshold**
- **calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent**
- **calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set**
- **calibrate-channel channel-set-optimization**
- **calibrate-channel channel-set-optimization neighbor-threshold**
- **calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent**
- **calibrate-channel channel-set-optimization neighbor-unmanaged-threshold percent-per-set**

5.1.13 calibrate-channel 2.4g channel-set-optimization neighbor-threshold

🕮 **メモ**:

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel 2.4 g channel-set-optimization neighbor-threshold *count*

undo calibrate-channel 2.4 g channel-set-optimization neighbor-threshold

デフォルト

10

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

count: 近隣数のしきい値を 1～1000 の範囲で設定します。

説明

calibrate-channel 2.4 g channel-set-optimization neighbor-threshold コマンドは近隣数のしきい値を設定します。

undo calibrate-channel 2.4 g channel-set-optimization neighbor-threshold コマンドはデフォルトに戻します。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

近隣数しきい値を 11 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-channel 2.4g channel-set-optimization neighbor-threshold 11

関連コマンド

- **calibrate-channel 2.4 g channel-set-optimization enable**
- **calibrate-channel channel-set-optimization**

5.1.14 calibrate-channel 2.4 g channel-set-optimization neighbor-unmanaged-threshold percent

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent *percent*

undo calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent

デフォルト

50%

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 管理対象外の周辺の比率のしきい値を 1～100 の範囲で設定します。

説明

calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent コマンドは管理対象外の近隣比率のしきい値を設定します。

undo calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent コマンドはデフォルトに戻します。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

管理対象外の近隣比率のしきい値を 20%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent 20

関連コマンド

- **calibrate-channel 2.4 g channel-set-optimization enable**
- **calibrate-channel channel-set-optimization**

5.1.15 calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set *percent*

undo channel-set-optimization neighbor-unmanaged-threshold percent-per-set

デフォルト

10%

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 単一のチャネルグループの管理対象外の近隣比率しきい値を 1～100 の範囲で設定します。

説明

calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set コマンドは 1 つのチャネルグループの管理対象外の近隣比率しきい値を設定します。

undo calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set コマンドはデフォルトに戻します。

RRM view の設定は、AP group RRM view および Global configuration view の設定より優先されます。

AP group RRM view の設定は、Global configuration view の設定より優先されます。

例

単一のチャネルグループの管理対象外の近隣比率しきい値を 20%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-channel 2.4g channel-set-optimization neighbor-unmanaged-threshold percent-per-set 20

5.1.16 calibrate-power 2.4g max

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g max *tx-power*

undo calibrate-power 2.4g max

デフォルト

2.4GHz 無線でサポートされる最大送信電力

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～27(dBm)の範囲で指定します。

説明

calibrate-power 2.4g max コマンドは TPC 実行後の無線に対して最大伝送電力を設定します。

undo calibrate-power 2.4g max コマンドはデフォルトに戻します。

このコマンドは、auto-TPC で設定できる無線の最大送信電力を設定します。

最大送信電力は、最小送信電力より小さい値を設定することはできません。

例

2.4GHz 無線の最大送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g max 15

5.1.17 calibrate-power 2.4g min

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g min *tx-power*

undo calibrate-power 2.4g min

デフォルト

6dBm

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～20(dBm)の範囲で指定します。

説明

calibrate-power 2.4g min コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power 2.4g min コマンドはデフォルトに戻します。

このコマンドは、TPC が実行された後も 2.4GHz 無線の送信電力がネットワーク要件を満たすことを保証します。

設定の優先度は RRM view、AP グループの RRM view、Global configuration view の順になっています。

例

2.4GHz 無線の最小送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g min 15

5.1.18 calibrate-power 2.4g coverage rssi-threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage rssi-threshold *rssi*

undo calibrate-power 2.4g coverage rssi-threshold

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

rssi: RSSI しきい値を 1～100 の範囲で指定します。パケットの RSSI が RSSI しきい値より低い場合、パケットは弱信号パケットと判別されます。

説明

calibrate-power 2.4g coverage rssi-threshold コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power 2.4g coverage rssi-threshold コマンドはデフォルトに戻します。

このコマンドは、2.4 GHz 無線での弱信号パケットとして判別する RSSI しきい値を設定します。

例

2.4GHz 無線の弱信号パケットと判別する RSSI しきい値に 80 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage rssi-threshold 80

関連コマンド

- **calibrate-power 2.4g coverage weak-signal-client ratio**

- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.19 calibrate-power 2.4g coverage weak-signal-client ratio

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-client ratio *percent*

undo calibrate-power 2.4g coverage weak-signal-client ratio

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号クライアント割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 2.4g coverage weak-signal-client ratio コマンドは 2.4 GHz 無線の弱信号クライアント割合のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-client ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、calibrate-power 2.4 g coverage weak-signal-client threshold コマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号クライアント割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-client ratio 30

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.20 calibrate-power 2.4g coverage weak-signal-client threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-client threshold *counts*

undo calibrate-power 2.4g coverage weak-signal-client threshold

デフォルト

3

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: 弱信号クライアント数のしきい値を 1～75 の範囲で指定します。

説明

calibrate-power 2.4g coverage weak-signal-client threshold コマンドは 2.4 GHz 無線の弱信号クライアント数のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-client threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、**calibrate-power 2.4g coverage weak-signal-client ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号クライアント数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-client threshold 20

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.21 calibrate-power 2.4g coverage weak-signal-packet ratio

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-packet ratio *percent*

undo calibrate-power 2.4g coverage weak-signal-packet ratio

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号パケット割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 2.4g coverage weak-signal-packet ratio コマンドは 2.4 GHz 無線の弱信号パケット割合のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-packet ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケット数が、calibrate-power 2.4 g coverage weak-signal-packet threshold コマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号パケット割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-packet ratio 30

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.22 calibrate-power 2.4g coverage weak-signal-packet threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 2.4g coverage weak-signal-packet threshold *counts*

undo calibrate-power 2.4g coverage weak-signal-packet threshold

デフォルト

5

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: クライアントの弱信号パケット数のしきい値を 1～255 の範囲で指定します。

説明

calibrate-power 2.4g coverage weak-signal-packet threshold コマンドは 2.4 GHz 無線の弱信号パケット数のしきい値を設定します。

undo calibrate-power 2.4g coverage weak-signal-packet threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケットの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、**calibrate-power 2.4g coverage weak-signal-packet ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

2.4GHz 無線の弱信号パケット数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 2.4g coverage weak-signal-packet threshold 20

関連コマンド

- **calibrate-power 2.4g coverage rssi-threshold**
- **calibrate-power 2.4g coverage weak-signal-client ratio**
- **calibrate-power 2.4g coverage weak-signal-client threshold**
- **calibrate-power 2.4g coverage weak-signal-packet ratio**
- **calibrate-power coverage enable**

5.1.23 calibrate-power 5g max

🕮 **メモ**:

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g max *tx-power*

undo calibrate-power 5g max

デフォルト

5GHz 無線でサポートされる最大送信電力

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～27(dBm)の範囲で指定します。

説明

calibrate-power 5g max コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power 5g max コマンドはデフォルトに戻します。

このコマンドは、auto-TPC で設定できる無線の最大送信電力を設定します。

最大送信電力は、最小送信電力より小さい値を設定することはできません。

例

5GHz 無線の最大送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g max 15

5.1.24 calibrate-power 5g min

🕮 **メモ**:

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g min *tx-power*

undo calibrate-power 5g min

デフォルト

11dBm

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～20(dBm)の範囲で指定します。

説明

calibrate-power 5g min コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power 5g min コマンドはデフォルトに戻します。

このコマンドは、TPC が実行された後も 5GHz 無線の送信電力がネットワーク要件を満たすことを保証します。

設定の優先度は RRM view、AP グループの RRM view、Global configuration view の順になっています。

例

5GHz 無線の最小送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g min 15

5.1.25 calibrate-power 5g coverage rssi-threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage rssi-threshold *rssi*

undo calibrate-power 5g coverage rssi-threshold

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

rssi: RSSI しきい値を 1～100 の範囲で指定します。パケットの RSSI が RSSI しきい値より低い場合、パケットは弱信号パケットと判別されます。

説明

calibrate-power 5g coverage rssi-threshold コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power 5g coverage rssi-threshold コマンドはデフォルトに戻します。

このコマンドは、5GHz 無線での弱信号パケットとして判別する RSSI しきい値を設定します。

例

5GHz 無線の弱信号パケットと判別する RSSI しきい値に 80 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage rssi-threshold 80

関連コマンド

- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.26 calibrate-power 5g coverage weak-signal-client ratio

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-client ratio *percent*

undo calibrate-power 5g coverage weak-signal-client ratio

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号クライアント割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 5g coverage weak-signal-client ratio コマンドは 5GHz 無線の弱信号クライアント割合のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-client ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、**calibrate-power 5g coverage weak-signal-client threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号クライアント割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-client ratio 30

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.27 calibrate-power 5g coverage weak-signal-client threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-client threshold *counts*

undo calibrate-power 5g coverage weak-signal-client threshold

デフォルト

3

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: 弱信号クライアント数のしきい値を 1～75 の範囲で指定します。

説明

calibrate-power 5g coverage weak-signal-client threshold コマンドは 5GHz 無線の弱信号クライアント数のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-client threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、**calibrate-power 5g coverage weak-signal-client ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号クライアント数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-client threshold 20

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.28 calibrate-power 5g coverage weak-signal-packet ratio

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-packet ratio *percent*

undo calibrate-power 5g coverage weak-signal-packet ratio

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号パケット割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 5g coverage weak-signal-packet ratio コマンドは 5GHz 無線の弱信号パケット割合のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-packet ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケット数が、**calibrate-power 5g coverage weak-signal-packet threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号パケット割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-packet ratio 30

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.29 calibrate-power 5g coverage weak-signal-packet threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 5g coverage weak-signal-packet threshold *counts*

undo calibrate-power 5g coverage weak-signal-packet threshold

デフォルト

5

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: クライアントの弱信号パケット数のしきい値を 1～255 の範囲で指定します。

説明

calibrate-power 5g coverage weak-signal-packet threshold コマンドは 5GHz 無線の弱信号パケット数のしきい値を設定します。

undo calibrate-power 5g coverage weak-signal-packet threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケットの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、**calibrate-power 5g coverage weak-signal-packet ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号パケット数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 5g coverage weak-signal-packet threshold 20

関連コマンド

- **calibrate-power 5g coverage rssi-threshold**
- **calibrate-power 5g coverage weak-signal-client ratio**
- **calibrate-power 5g coverage weak-signal-client threshold**
- **calibrate-power 5g coverage weak-signal-packet ratio**
- **calibrate-power coverage enable**

5.1.30 calibrate-power 6g max

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g max *tx-power*

undo calibrate-power 6g max

デフォルト

6GHz 無線でサポートされる最大送信電力

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～27(dBm)の範囲で指定します。

説明

calibrate-power 6g max コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power 6g max コマンドはデフォルトに戻します。

このコマンドを設定すると、無線の伝送電力は設定値を超えなくなります。

最大送信電力は、最小送信電力より小さい値を設定することはできません。

例

6GHz 無線の最大送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g max 15

5.1.31 calibrate-power 6g min

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g min *tx-power*

undo calibrate-power 6g min

デフォルト

11dBm

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

tx-power: 最大送信電力を 1～20(dBm)の範囲で指定します。

説明

calibrate-power 6g min コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power 6g min コマンドはデフォルトに戻します。

このコマンドは、TPC が実行された後も 6GHz 無線の送信電力がネットワーク要件を満たすことを保証します。

設定の優先度は RRM view、AP グループの RRM view、Global configuration view の順になっています。

例

6GHz 無線の最小送信電力を 15 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g min 15

5.1.32 calibrate-power 6g coverage rssi-threshold

🕮 メモ：

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage rssi-threshold *rssi*

undo calibrate-power 6g coverage rssi-threshold

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

rssi: RSSI しきい値を 1～100 の範囲で指定します。パケットの RSSI が RSSI しきい値より低い場合、パケットは弱信号パケットと判別されます。

説明

calibrate-power 6g coverage rssi-threshold コマンドは TPC 実行後の無線に対して最小伝送電力を設定します。

undo calibrate-power 6g coverage rssi-threshold コマンドはデフォルトに戻します。

このコマンドは、6GHz 無線での弱信号パケットとして判別する RSSI しきい値を設定します。

例

6GHz 無線の弱信号パケットと判別する RSSI しきい値に 80 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage rssi-threshold 80

関連コマンド

- **calibrate-power 6g coverage weak-signal-client ratio**
- **calibrate-power 6g coverage weak-signal-client threshold**
- **calibrate-power 6g coverage weak-signal-packet ratio**
- **calibrate-power 6g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.33 calibrate-power 6g coverage weak-signal-client ratio

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage weak-signal-client ratio *percent*

undo calibrate-power 6g coverage weak-signal-client ratio

デフォルト

25

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号クライアント割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 6g coverage weak-signal-client ratio コマンドは 6GHz 無線の弱信号クライアント割合のしきい値を設定します。

undo calibrate-power 6g coverage weak-signal-client ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、**calibrate-power 6g coverage weak-signal-client threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

6GHz 無線の弱信号クライアント割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage weak-signal-client ratio 30

関連コマンド

- **calibrate-power 6g coverage rssi-threshold**
- **calibrate-power 6g coverage weak-signal-client threshold**
- **calibrate-power 6g coverage weak-signal-packet ratio**
- **calibrate-power 6g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.34 calibrate-power 6g coverage weak-signal-client threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage weak-signal-client threshold *counts*

undo calibrate-power 6g coverage weak-signal-client threshold

デフォルト

3

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: 弱信号クライアント数のしきい値を 1～75 の範囲で指定します。

説明

calibrate-power 6g coverage weak-signal-client threshold コマンドは 6GHz 無線の弱信号クライアント数のしきい値を設定します。

undo calibrate-power 6g coverage weak-signal-client threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱信号クライアントの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- 無線に関連付けられた弱信号クライアントの割合が、**calibrate-power 6g coverage weak-signal-client ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

5GHz 無線の弱信号クライアント数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage weak-signal-client threshold 20

関連コマンド

- **calibrate-power 6g coverage rssi-threshold**
- **calibrate-power 6g coverage weak-signal-client ratio**
- **calibrate-power 6g coverage weak-signal-packet ratio**
- **calibrate-power 6g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.35 calibrate-power 6g coverage weak-signal-packet ratio

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage weak-signal-packet ratio *percent*

undo calibrate-power 6g coverage weak-signal-packet ratio

デフォルト

20

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

percent: 弱信号パケット割合のしきい値を 1～100 の範囲で指定します。単位はパーセントです。

説明

calibrate-power 6g coverage weak-signal-packet ratio コマンドは 6GHz 無線の弱信号パケット割合のしきい値を設定します。

undo calibrate-power 6g coverage weak-signal-packet ratio コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケット数が、**calibrate-power 6g coverage weak-signal-packet threshold** コマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、このコマンドで設定した割合しきい値に達するか、それを超えた場合。

例

6GHz 無線の弱信号パケット割合のしきい値を 30%に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage weak-signal-packet ratio 30

関連コマンド

- **calibrate-power 6g coverage rssi-threshold**
- **calibrate-power 6g coverage weak-signal-client ratio**
- **calibrate-power 6g coverage weak-signal-client threshold**
- **calibrate-power 6g coverage weak-signal-packet threshold**
- **calibrate-power coverage enable**

5.1.36 calibrate-power 6g coverage weak-signal-packet threshold

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

calibrate-power 6g coverage weak-signal-packet threshold *counts*

undo calibrate-power 6g coverage weak-signal-packet threshold

デフォルト

5

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

counts: クライアントの弱信号パケット数のしきい値を 1～255 の範囲で指定します。

説明

calibrate-power 6g coverage weak-signal-packet threshold コマンドは 6GHz 無線の弱信号パケット数のしきい値を設定します。

undo calibrate-power 6g coverage weak-signal-packet threshold コマンドはデフォルトに戻します。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- クライアントの弱信号パケットの数が、このコマンドで設定したしきい値に達するか、それを超えた場合。
- クライアントの弱信号パケットの割合が、**calibrate-power 6g coverage weak-signal-packet ratio** コマンドで設定した割合しきい値に達するか、それを超えた場合。

例

6GHz 無線の弱信号パケット数のしきい値を 20 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power 6g coverage weak-signal-packet threshold 20

関連コマンド

- **calibrate-power 6g coverage rssi-threshold**
- **calibrate-power 6g coverage weak-signal-client ratio**
- **calibrate-power 6g coverage weak-signal-client threshold**
- **calibrate-power 6g coverage weak-signal-packet ratio**
- **calibrate-power coverage enable**

5.1.37 calibrate-power coverage enable

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

Radio view または AP グループの Radio view:

calibrate-power coverage { disable | enable }

undo calibrate-power coverage

Global configuration View:

calibrate-power coverage enable { 2.4g | 5g | 6g | all }

undo calibrate-power coverage enable { 2.4g | 5g | 6g | all }

デフォルト

Radio view：AP group view の設定を使用します。

AP group Radio view：global configuration view の設定を使用します。

Global configuration view：無効

View

Radio view

AP group Radio view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

2.4g: 2.4GHz 無線を指定します。

5g: 5GHz 無線を指定します。

6g: 6GHz 無線を指定します。

all: ソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでは 2.4GHz 無線、5GHz 無線、6GHz 無線のすべてを指定します。

ソフトウェアバージョン 7.2.73 を含む以前のソフトウェアでは 2.4GHz 無線と 5GHz 無線両方を指定します。

説明

calibrate-power coverage enable コマンドは死角検出を有効にします。

calibrate-power coverage disable コマンドは死角検出を無効にします。

undo calibrate-power coverage コマンドはデフォルトに戻します。

この機能により、AC は無線信号カバレッジに死角 (または弱い信号領域) が存在するかどうかを判断できます。死角が検出された場合、AC は auto-TPC を実行するときに対応する AP の送信電力を増加させます。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱い信号クライアントの数が、しきい値に達するか、または超えている場合。
- 無線に関連付けられた弱い信号クライアントの割合がしきい値に達するか、それを超えている場合。

AC は、次の条件が満たされた場合に、クライアントが弱信号クライアントであると判断します。

- クライアントの弱信号パケット数がしきい値に達するか、またはしきい値を超えた場合。
- クライアントの弱信号パケットの割合がしきい値に達するか、それを超えた場合。

パケットの RSSI が RSSI しきい値より低い場合、そのパケットは弱い信号パケットと見なされます。

例

ap1 と名付けた AP の Radio3 で死角検出を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 3

[AC-wlan-ap-ap1-radio-3] calibrate-power coverage enable

group1 と名付けた AP group のモデル **QX-W1020** の無線 3 で、死角検出を有効にします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 3

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-3] calibrate-power coverage enable

#グローバルで 2.4GHz 無線の死角検出を有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power coverage enable 2.4g

関連コマンド

- calibrate-power 2.4g coverage rssi-threshold
- calibrate-power 2.4g coverage weak-signal-client ratio
- calibrate-power 2.4g coverage weak-signal-client threshold
- calibrate-power 2.4g coverage weak-signal-packet ratio
- calibrate-power 2.4g coverage weak-signal-packet threshold
- calibrate-power 5g coverage rssi-threshold
- calibrate-power 5g coverage weak-signal-client ratio
- calibrate-power 5g coverage weak-signal-client threshold
- calibrate-power 5g coverage weak-signal-packet ratio
- calibrate-power 5g coverage weak-signal-packet threshold
- calibrate-power 6g coverage rssi-threshold
- calibrate-power 6g coverage weak-signal-client ratio
- calibrate-power 6g coverage weak-signal-client threshold
- calibrate-power 6g coverage weak-signal-packet ratio
- calibrate-power 6g coverage weak-signal-packet threshold

5.1.38 calibrate-power min

Syntax

calibrate-power min *tx-power*

undo calibrate-power min

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :グローバル構成を継承します。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

パラメータ

tx-power:Radio の最小送信電力は、 1～20 の範囲の値をとり、単位は dBm である。

説明

calibrate-power min コマンドは、Radio の最小送信電力を設定するために使用されます。

undo calibrate-power min コマンドを使用して、デフォルトの状態を復元します。

自動電力調整が完了しても、Radio の送信電力は、このコマンドで設定した値を下回ることはありません。

RRM view の下の構成は、AP group's RRM view の下の構成よりも優先され、AP group's RRM view の下の構成は、グローバルビューの下の構成よりも優先されます。

例

#設定 Radio の最小送信電力は 15 dBm です。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power min 15

#設定 Radio の最小送信電力は 15 dBm です。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power min 15

5.1.39 calibrate-power mode

Syntax

calibrate-power mode { **coverage** | **custom** | **density** }

undo calibrate-power mode

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :自動電力調整モードはカスタムモードです。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

パラメータ

coverage:カバレッジモード:AP 信号のカバレッジ拡大に偏った電力調整方式で、 AP 数の少ない無線環境に適している。

custom:AC が手動で設定した電力調整パラメータに基づいて電力調整を行うカスタムモード。

density:高密モードは、 AP 間の信号干渉回避に偏った電力調整方式であり、 AP 数が多く、信号重畳領域が多い無線環境に適している。

説明

calibrate-power mode コマンドを使用して、自動電力調整モードを設定します。

undo calibrate-power mode コマンドを使用して、デフォルトの状態を復元します。

オーバーレイモードと高密度モードはシステム定義の電力調整パラメータを使用して自動電力調整を行い、カスタムモードは手動で設定した電力調整パラメータを使用して自動電力調整を行います。

例

#自動電力調整モードをオーバーレイモードに設定します。(RRM view)

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power mode coverage

#自動電力調整モードを高密度モードに設定します。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power mode density

5.1.40 calibrate-power self-decisive

Syntax

RRM view/ AP group's RRM view :

calibrate-power self-decisive { **disable** | **enable** }

undo calibrate-power self-decisive

Global configuration view:

calibrate-power self-decisive enable { **2.4g** | **5g** | **6g** | **all** }

undo calibrate-power self-decisive { **2.4g** | **5g** | **6g** | **all** }

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :グローバル構成を継承します。

Global Configuration View: auto-TPC がオフになっています。

View

RRM view

AP group's RRM view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

2.4g:すべての AP の 2.4 GHz 帯無線周波数の自動電力調整機能のオン/オフを切り替えます。

5g:すべての AP の 5 GHz 帯無線周波数の自動電力調整機能のオン/オフを切り替えます。

6g:すべての AP の 6 GHz 帯無線周波数の自動電力調整機能のオン/オフを切り替えます。

🕮 **メモ：**

6g パラメータはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

---

all: ソフトウェアバージョン 9.4.05 のソフトウェアではすべての AP の 2.4 GHz および 5 GHz 帯域無線の自動電力調整機能のオン/オフを切り替えます。ソフトウェアバージョン 9.4.09 を含む以降のソフトウェアでは、すべての AP の 2.4GHz、5GHz、6GHz 帯域無線の自動電力調整機能のオン/オフを切り替えます。

説明

calibrate-power self-decisive enable コマンドを使用して、自動電力調整をオンにします。

calibrate-power self-decisive disable コマンドを使用して、自動電力調整をオフにします。

undo calibrate-power self-decisive コマンドを使用して、デフォルトの状態を復元します。

自動電力調整をオンにすると、AC は各自動電力調整サイクルが完了するたびに電力調整プロセスを開始します。

RF の最大送信電力が設定されている場合、現在の RF の自動電力調整機能は無効になります。

例

#自動電源調整をオンにします。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power self-decisive enable

#自動電源調整をオンにします。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power self-decisive enable

#すべての AP の 2.4 GHz および 5 GHz 帯域無線周波数の自動電力調整機能をオンにします。(Global configuration view)

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] calibrate-power self-decisive enable all

関連コマンド

- **wlan rrm calibration-power interval**

5.1.41 calibrate-power threshold

Syntax

calibrate-power threshold *value*

undo calibrate-power threshold

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :グローバル構成を継承します。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

パラメータ

threshold *value*:パワー調整しきい値は 1~196 の範囲で、代表パワー範囲は-1 dBm~-196dBm です。すなわち、パワーしきい値が大きいほど、パワー値が小さいことを示す。

説明

calibrate-power threshold コマンドを使用して、電力調整しきい値を設定します。

undo calibrate-power threshold コマンドを使用して、デフォルトの状態を復元します。

合理的に閾値を設定する必要があり、AP 上の Radio が比較的に大きいカバー範囲を有し、弱い信号が出現しないことを保証し、正常な使用需要を満足し、同時に AP 間の相互干渉を減少する。

RRM view の下の構成は、AP group's RRM view の下の構成よりも優先され、AP group's RRM view の下の構成は、グローバルビューの下の構成よりも優先されます。

例

#設定電力調整しきい値は-70 dBm です。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power threshold 70

#設定電力調整しきい値は-70 dBm です。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] calibrate-power threshold 70

5.1.42 channel holddown-time

Syntax

channel holddown-time *minutes*

undo channel holddown-time

デフォルト

チャネル保持時間は 720 分です。

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

minutes:チャネル保持時間は分単位で 10~1440 の値をとります。

説明

チャネルのキープアライブ時間を設定するには、**channel holddown-time** コマンドを使用します。

undo channel holddown-time コマンドを使用して、デフォルトの状態を復元します。

RRM 保持調整グループに参加する無線周波数チャネルは、各調整後のチャネル保持時間の間、調整されない。

例

#RRM キープアライブグループ 10 のチャネルキープアライブ時間を 600 分に設定します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] channel holddown-time 600

5.1.43 crc-error-threshold

Syntax

crc-error-threshold *percent*

undo crc-error-threshold

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :グローバル構成を継承します。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

パラメータ

percent:CRC エラーしきい値。パーセントで 0~100 の値をとります。0 時の値は、自動チャネル調整で CRC エラーしきい値が考慮されないことを示します。

説明

CRC エラーしきい値を設定するには、**crc-error-threshold** コマンドを使用します。

undo crc-error-threshold コマンドを使用して、デフォルトの状態を復元します。

CRC エラーしきい値は、自動チャネル調整をトリガする条件の 1 つであり、AC がチャネル内の CRC エラーフレームの全 802.11 フレームに対する割合が設定値を超えたことを検出すると、チャネル調整がトリガされます。

RRM view の下の CRC エラーしきい値構成は、AP group's RRM view の下の構成よりも優先され、AP group's RRM view の下の CRC エラーしきい値構成は、グローバルビューの下の構成よりも優先されます。

例

#CRC エラーしきい値を 50 に設定します。CRC エラー率が 50%以上になると、自動チャネル調整がトリガされます。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] crc-error-threshold 50

#CRC エラーしきい値を 50 に設定します。CRC エラー率が 50%以上になると、自動チャネル調整がトリガされます。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] crc-error-threshold 50

5.1.44 description

Syntax

description *text*

undo description

デフォルト

RRM 保持調整グループの説明情報がありません。

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

text:RRM は、大文字と小文字を区別する 1~64 文字の文字列で、調整グループの説明を保持します。

説明

description コマンドは、RRM ホールドアップ調整グループの説明情報を設定します。

undo description コマンドを使用して、デフォルトの状態を復元します。

例

#RRM ホールドアップの設定調整グループ 10 の説明情報は office です。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] description office

5.1.45 display wlan rrm baseline

Syntax

display wlan rrm baseline { **all** | **name** *baseline-name* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:保存されているすべての RF 動作パラメータのベースライン情報を表示します。

name *baseline-name*:保存された RF 動作パラメータのベースライン情報を表示します。ここで、baseline-name はベースラインの名前を表します。は 1~32 文字の文字列で、大文字と小文字は区別されません。

verbose:RF 動作パラメータのベースラインの詳細を表示します。このパラメータを指定しないと、ベースラインのサマリー情報が表示されます。

説明

display wlan rrm baseline コマンドは、RF 動作パラメータのベースラインに関する情報を表示します。

現在のユーザが location 権限を持っていない AP の無線周波数情報が無線周波数動作パラメータベースラインに保存されている場合、そのユーザは無線周波数動作パラメータベースラインを表示できません。

例

#保存されているすべてのベースラインのサマリー情報を表示します。

<AC> display wlan rrm baseline all

Baseline name:apbaseline

Radio range:AP

Created at:2015-06-22 19:56:31

Baseline name:groupbaseline

Radio range:AP group

Created at:2015-06-22 19:56:12

Baseline name:globalbaseline

Radio range:Global

Created at:2015-06-22 19:55:12

表 5-1 display wlan rrm baseline all コマンドの表示情報の説明

フィールド	説明
Baseline name	RF動作パラメータのベースラインの名前
Radio range	RF動作パラメータのベースラインに保存されているRFの範囲。以下の値を取ります。 • AP:AP の無線周波数 • AP group:AP グループ内の無線 • Global:AC 上のすべての AP の無線周波数
Created at	RF動作パラメータベースラインの作成時間

#保存されているすべての RF 動作パラメータのベースラインの詳細を表示します。

<AC> display wlan rrm baseline all verbose

```
------------------------------------------------------------------------------
-
 Baseline name : apbaseline
 Radio range   : AP
 Created at    : 2015-06-22 19:56:31
------------------------------------------------------------------------------
-
 APName             RadioID RadioType Bandwidth Channel Power RegionCode
------------------------------------------------------------------------------
-
 ap1                2       dot11gn   20        13      20    CN
------------------------------------------------------------------------------
-


------------------------------------------------------------------------------
-
 Baseline name : groupbaseline
 Radio range   : AP group
 Created at    : 2015-06-22 19:56:12
------------------------------------------------------------------------------
-
 APName             RadioID RadioType Bandwidth Channel Power RegionCode
------------------------------------------------------------------------------
-
 ap1                1       dot11an   40        157     20    CN
 ap2                1       dot11an   40        149     20    CN
------------------------------------------------------------------------------
-
```

```
------------------------------------------------------------------------------
-
 Baseline name : globalbaseline
 Radio range   : Global
 Created at    : 2015-06-22 19:55:12
------------------------------------------------------------------------------
-
 APName             RadioID RadioType Bandwidth Channel Power RegionCode
------------------------------------------------------------------------------
-
 ap1                1       dot11an   40        149     20    CN
 ap1                2       dot11gn   20        13      20    CN
 ap2                1       dot11an   40        149     20    CN
 ap2                2       dot11gn   20        1       20    CN
------------------------------------------------------------------------------
-
```

表 5-2 display wlan rrm baseline all verbose コマンドの表示情報の説明

フィールド	説明
Baseline name	RF動作パラメータのベースラインの名前
Radio range	RF動作パラメータのベースラインに保存されているRFの範囲。以下の値を取ります。 • AP:AP の無線周波数 • AP group:AP グループ内の無線 • Global:AC 上のすべての AP の無線周波数
Created at	RF動作パラメータベースラインの作成時間
APName	APの名前
RadioID	無線周波数番号
RadioType	無線周波数タイプ
Bandwidth	無線帯域幅
Channel	無線周波数チャネル
Power	無線周波数の送信電力:dBm
RegionCode	APのエリアコード

5.1.46 display wlan rrm baseline apply-history

Syntax

display wlan rrm baseline apply-history [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose:RF 動作パラメータのベースラインの詳細な履歴情報。このパラメータを指定しない場合、RF 動作パラメータのベースラインに関する簡単な履歴情報が表示されます。

説明

display wlan rrm baseline apply-history コマンドを使用して、アプリケーションの RF 動作パラメータのベースラインに関する履歴情報を表示します。

このコマンドは、無線周波動作パラメータのベースラインを最後に 10 回適用した履歴を表示し、10 回未満の場合はすべて表示します。

例

#アプリケーションの RF 動作パラメータのベースラインに関する簡単な履歴情報を表示します。

<AC> display wlan rrm baseline apply-history
Name : global1
Applied at : 2016-01-23 12:19:50
Applied to : global

#アプリケーションの RF 動作パラメータのベースラインの詳細な履歴情報を表示します。

<AC> display wlan rrm baseline apply-history verbose
Name : global1
Applied at : 2016-01-23 12:19:50
Applied to : global
Radios : 6
Success : 4
Failure : 2
Failure reason
Radio doesn't exist : 0
Radio is down : 0
Mismatching radio type : 0
Mismatching region code : 1
Ineffective service template : 0
Illegal channel : 0
Mismatching bandwidth : 1
Channel locked : 0
Channel fixed : 0
Within channel holddown time : 0
Mismatching channel gap policy: 0
Power locked : 0
Within power holddown time : 0

Power lower than min. power ：0

Power greater than max. power：0

表 5-3 display wlan rrm baseline apply-history コマンドの表示情報の説明

フィールド	説明
Name	RF動作パラメータのベースラインの名前
Applied at	無線周波数作動パラメータベースラインの応用時間
Applied to	RF動作パラメータのベースラインの適用範囲は次のとおりです。 • ap:指定された AP に適用 • apgroup:指定された AP グループに適用されます。 • global:グローバルに適用
Radio count	RF動作パラメータベースラインの総RF数
Success	RF動作パラメータベースラインアプリケーションが成功したRF数
Failure	RF動作パラメータベースラインアプリケーションに失敗したRFの数
Failure reason	RF動作パラメータベースラインの適用失敗数
Radio doesn't exist	無線周波数がありません
Radio is down	無線周波数ステータスがDown
Mismatching radio type	RF動作パラメータのベースラインに保存されているRFタイプが、実際のRFタイプと一致しません。
Mismatching region code	RF動作パラメータのベースラインに保存されているAPのエリアコードが、実際の状況と一致しません。
Ineffective service template	ワイヤレスサービスが有効になっていません
Illegal channel	無線周波数動作パラメータのベースラインに保存された無線周波数動作チャネルの不正
Mismatching bandwidth	無線周波数動作パラメータのベースラインに保存された無線周波数帯域幅が実際の無線周波数帯域幅と一致しない
Channel locked	作業チャネルがロックされています
Channel fixed	無線周波数の動作チャネルが固定値に手動で設定されている
Within channel holddown time	現在の動作チャネルはチャネル保持調整期間中です
Mismatching channel gap policy	無線周波数動作パラメータのベースラインに保存された無線周波数動作チャネルは、チャネル間隔ポリシーによって選択されたチャネルと一致しません。
Power locked	RF電力がロックされている
Within power holddown time	現在の無線周波電力は電力保持調整期間中です
Power lower than min.power	RF動作パラメータベースラインに保存されているRF電力は、設定されている最小送信電力よりも小さくなります。
Power greater than max.power	RF動作パラメータベースラインに保存されているRF電力が、設定されている最大送信電力を超えています。

関連コマンド

- **wlan rrm baseline apply name**

5.1.47 display wlan rrm-calibration-group

Syntax

display wlan rrm-calibration-group { **all** | *group-id* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての RRM は調整グループを保持します。

group-id:RRM は調整グループの ID を 1~128 の範囲の値で保持します。

説明

display wlan rrm-calibration-group コマンドを使用して、RRM ホールドアップ調整グループに関する情報を表示します。

例

#RRM ホールド調整グループ 10 に関する情報を表示する。

<AC> display wlan rrm-calibration-group 10

RRM Calibration Group Information

Group ID : 10

Description : office

Channel holddown time : 720 minutes

Power holddown time : 60 minutes

Location name : default-location

Group members : ap4-radio2, ap3-radio2

表 5-4 display wlan rrm-calibration-group コマンドの表示情報の説明

フィールド	説明
Group ID	RRMは、調整グループのIDを保持します。
Description	RRMは、調整グループの説明情報を保持します。
Channel holddown time	チャネル持続時間
Power holddown time	電力保持時間
Location name	地域識別名
Group members	RRMキープアライブグループに参加Radio

5.1.48 display wlan rrm high-density filter history

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

display wlan rrm high-density filter history

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan rrm high-density filter history コマンドを使用して、高密度シナリオでシャットダウンできる AP に関するフィルタ履歴を表示します。

このコマンドは、最新の 5 つのフィルタリング操作の結果を表示できます。ベストプラクティスとして、高密度シナリオで無線干渉を減らすために、フィルタ結果に基づいて AP を手動で無効にします。

例

#高密度シナリオでシャットダウンできる AP に関するフィルタ履歴を表示します。

<AC> display wlan rrm high-density filter history

```
Time           : 2019-06-22 19:55:12
Range          : group1 (AP group)
Frequency-band: 2.4GHz/5GHz
2.4GHz shutdown list :
AP name     RID Channel
ap1          2    1
ap2          2    6
ap3          2    11

5GHz shutdown list :
AP name      RID  Channel
ap1          1    36
ap2          1    40
ap3          1    44
----------------------------------------------------------------
```

```
Time      : 2019-06-29 09:59:16
Range     : All APs
Radio type: 5GHz
2.4GHz shutdown list :

5GHz shutdown list :
AP name      RID  Channel
ap11         1    36
ap12         1    40
ap13         1    44
------------------------------------------------------------------
```

表 5-5 コマンドの表示情報の説明

フィールド	説明
Time	フィルタ操作が実行される時間
Range	フィルタするAP範囲。次のオプションがあります。 ● APグループ名 ● 全てのAP
Frequency-band	フィルタするラジオタイプ。次のオプションがあります。 ● 2.4GHz ● 5GHz ● 2.4GHz/5GHz ● 6GHz
2.4GHz shutdown list	シャットダウンできる、フィルタリングされた2.4 GHz無線APのリスト
5GHz shutdown list	シャットダウンできる、フィルタリングされた5 GHz無線APのリスト
RID	無線ID
Channel	無線の動作チャネル

5.1.49 display wlan rrm-history ap

Syntax

display wlan rrm-history ap { **all** | **name** *ap-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての AP。

name *ap-name*:AP 名。1~64 文字の文字列で、英数字、アンダースコア、.、[」 、 「]、/、-を使用できます。大文字と小文字は区別されます。

説明

display wlan rrm-history ap コマンドを使用して、RRM 調整履歴情報を表示します。

このコマンドは、AP で最後に 3 回変更されたチャネルまたは電力の詳細を表示します。表示出力は変化時間、触発原因、電力、干渉などのパラメータを含む。

例

#ap 1 の RRM 履歴情報を表示します。

```
<AC> display wlan rrm-history ap name ap1
                    AP RRM History
------------------------------------------------------------------------------
 Flags：I - Interference,   P - Packets discarded,   F - Retransmission,
       R - Radar select,   C - Coverage,          B - Channelbusy
       M – Manual         D – Bandwidth          O - Others
------------------------------------------------------------------------------


                  AP RRM History：ap1
------------------------------------------------------------------------------
 Radio：1                          Basic BSSID：000f-e2ff-7700
------------------------------------------------------------------------------
      Ch  Power BW    Load Util Intf   Reason    Date        Time
        (dBm) (MHz) (%)  (%)  (%)            (yyyy-mm-dd) (hh:mm:ss)
------------------------------------------------------------------------------
 Before 36   20   20    24   2    21    -P------- 2014-07-07   17:31:50
 After  40   20   20    9    0    8     -         -           -
------------------------------------------------------------------------------
 Before 40   20   20    54   1    53    IP------- 2014-07-08   12:19:50
 After  36   20   20    10   0    10    -         -           -
------------------------------------------------------------------------------
 Before 36   20   20    29   1    28    -------D- 2014-07-08   12:59:50
 After  36   20   40    30   0    29    -         -           -
------------------------------------------------------------------------------
```

表 5-6 display wlan rrm-history コマンドの表示情報の説明

フィールド	説明
Radio	APのRadio ID
Basic BSSID	基本サービスセットID
Ch	Radioの動作チャネル
Power (dBm)	Radioの送信電力。単位はdBmです。
BW (MHz)	Radioの動作周波数はMHz
Load (%)	チャネルの負荷。パーセントで表されます。
Util (%)	チャネルの使用率、パーセントで表示

フィールド	説明
Intf (%)	チャネルで検出された干渉の割合
Reason	調整の理由は、次のとおりです。 • I:干渉 • P:ドロップ • F:再送信 • R:レーダー信号を回避した後、より良いチャネルを選択する • C:信号カバー • B:チャネルビジー • M:手動トリガ • D:帯域幅の調整 • O:その他の原因
Date	修正日
Time	調整時間

5.1.50 display wlan rrm-status ap

Syntax

display wlan rrm-status ap { **all** | **name** *ap-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべての AP。

name *ap-name*:AP 名。1~64 文字の文字列で、英数字、アンダースコア、.、[」 、 「]、/、-を使用できます。大文字と小文字は区別されます。

説明

display wlan rrm-status ap コマンドを使用して、AP の無線周波数の RRM 詳細を表示します。

チャネルと電力の調整がオフの場合、このコマンドを実行すると、AP 上の Radio の動作チャネルと電力レベルのみが表示され、干渉やネイバーの数などの他の情報は表示されません。

例

#ap 1 のチャネルと電力調整の詳細を表示します。

```
<AC> display wlan rrm-status ap name ap1
                AP RRM Profile：ap1
--------------------------------------------------------------------------------
 Radio  ：1                     Basic BSSID   ：70f9-6d31-2fe0
 Channel：157                     Tx Power (dBm)：18
--------------------------------------------------------------------------------
   Ch   Nbrs  Load  Util  Intf  PER   Retry  Radar    Last Detected At
          (%)   (%)   (%)   (%)   (%)
--------------------------------------------------------------------------------
   36   0     0     -     0     0     -      -        2020-04-10 09:35:01
   40   0     0     -     0     0     -      -        2020-04-10 09:35:01
   44   0     0     -     0     0     -      -        2020-04-10 09:35:01
   48   0     0     -     0     0     -      -        2020-04-10 09:35:01
   52   0     0     -     0     0     -      -        2020-04-10 09:35:01
   56   0     0     -     0     0     -      -        2020-04-10 09:35:01
   60   0     0     -     0     0     -      -        2020-04-10 09:35:01
   64   0     0     -     0     0     -      -        2020-04-10 09:35:01
   100  0     0     -     0     0     -      -        2020-04-10 09:35:01
   104  0     0     -     0     0     -      -        2020-04-10 09:35:01
   108  0     0     -     0     0     -      -        2020-04-10 09:35:01
   112  0     0     -     0     0     -      -        2020-04-10 09:35:01
   116  0     0     -     0     0     -      -        2020-04-10 09:35:01
   132  0     0     -     0     0     -      -        2020-04-10 09:35:01
   136  0     0     -     0     0     -      -        2020-04-10 09:35:01
   140  0     0     -     0     0     -      -        2020-04-10 09:35:01
   149  1     0     -     0     0     -      -        2020-04-10 09:35:01
   153  4     0     -     0     0     -      -        2020-04-10 09:35:01
   157  0     0     0     0     0     0      -        2020-04-10 09:35:01
   161  2     0     -     0     0     -      -        2020-04-10 09:35:01
   165  0     0     -     0     0     -      -        2020-04-10 09:35:01
--------------------------------------------------------------------------------
   Nbr-MACAddress   Ch   Intf   SignalStrength  Type        Last Detected At
                    (%)  (dBm)
--------------------------------------------------------------------------------
   000f-e212-ff01   161  0      -60             Unmanaged   2020-04-10 09:39:03
   5866-ba74-e461   153  0      -72             Unmanaged   2020-04-10 09:39:03
   70f9-6d30-9020   153  0      -40             Managed     2020-04-10 09:39:03
   70f9-6d31-3080   149  0      -54             Managed     2020-04-10 09:39:03
   70f9-6d31-34e0   161  0      -59             Managed     2020-04-10 09:39:03
   7425-8a86-bbe0   153  0      -48             Unmanaged   2020-04-10 09:39:03
   7425-8a86-c720   153  0      -63             Unmanaged   2020-04-10 09:39:03
--------------------------------------------------------------------------------
 Radio  ：2                     Basic BSSID   ：70f9-6d31-2ff0
```

```
Channel：1                    Tx Power (dBm)：19
--------------------------------------------------------------------------------
  Ch   Nbrs   Load   Util   Intf   PER   Retry   Radar    Last Detected At
              (%)    (%)    (%)    (%)   (%)
--------------------------------------------------------------------------------
  1    6      4      0      4      0     0       -        2020-04-10 09:33:06
  6    4      2      -      2      0     -       -        2020-04-10 09:33:06
  11   6      2      -      2      0     -       -        2020-04-10 09:33:06
--------------------------------------------------------------------------------
  Nbr-MACAddress   Ch    Intf   SignalStrength  Type        Last Detected At
                         (%)    (dBm)
--------------------------------------------------------------------------------
  000f-e212-ff11   1     49     -77             Unmanaged   2020-04-10 09:31:05
  0023-89e1-ed00   11    0      -87             Unmanaged   2020-04-10 09:31:05
  006a-55f6-ae10   1     57     -88             Unmanaged   2020-04-10 09:31:05
  5866-ba64-aa31   1     10     -60             Unmanaged   2020-04-10 09:31:05
  5866-ba74-e471   6     0      -76             Unmanaged   2020-04-10 09:31:05
  5866-baa9-a610   11    0      -62             Unmanaged   2020-04-10 09:31:05
  70f9-6d30-9030   6     0      -63             Managed     2020-04-10 09:31:05
  70f9-6d31-3090   1     51     -86             Managed     2020-04-10 09:31:05
  70f9-6d31-34f0   6     0      -85             Managed     2020-04-10 09:33:09
  7425-8a86-bbf0   6     0      -73             Unmanaged   2020-04-10 09:33:09
  7425-8a86-c731   11    0      -93             Unmanaged   2020-04-10 09:33:09
  80f6-2ec0-3330   11    0      -76             Unmanaged   2020-04-10 09:33:09
  80f6-2ec0-3331   11    0      -73             Unmanaged   2020-04-10 09:33:09
  80f6-2edd-d2d0   1     40     -60             Unmanaged   2020-04-10 09:33:09
  80f6-2edd-d2d1   1     44     -68             Unmanaged   2020-04-10 09:33:09
  80f6-2ede-0b30   11    0      -74             Unmanaged   2020-04-10 09:33:09
```

表 5-7 display wlan rrm-status コマンドの表示情報の説明

フィールド	説明
Radio	APのRadio ID
Basic BSSID	基本サービスセットID
Channel	Radio現在の動作チャネル
Tx Power	Radioの送信電力
Ch	Radioサポートされている動作チャネル
Nbrs	チャネル内のネイバーRadioの数
Load	チャネルの負荷。パーセントで表されます。チャネルの負荷とは、そのチャネル上でAPがメッセージを送信/受信するクライアントのメッセージと干渉であり、ここで干渉とは、そのAPが他のAPやクライアントから送信されるエラーメッセージを受信することである.
Util	チャネル使用率。パーセントで表示されます。チャネル利用率とは、そのチャネル上でAPがメッセージを送信/受信するクライアントのメッセージである.
Intf	チャネルで検出された干渉の割合
PER	チャネルで検出されたビット誤り率。パーセントで表されます。
Retry	チャネルで検出された再送率。パーセントで表されます。

フィールド	説明
Radar	レーダー検出状態: • -レーダーが検出されなかったことを示します • Detected はレーダーが検出されたことを示します。
Nbr-MACAddress	ネイバーAPのRadioインタフェースのMACアドレス
SignalStrength	dBm単位で検出されたネイバーRadioの信号強度
Type	APタイプ: • Unmanaged:この AP の Radio が検出できる非ネイバーRadio • Managed:この AP の Radio が検出できるネイバーRadio
Last Detected At	チャネルおよびネイバーの有効データが最後に検出された時刻

5.1.51 interference-threshold

Syntax

interference-threshold *percent*

undo interference-threshold

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :チャネル干渉しきい値は 0 です。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

パラメータ

percent:チャネル干渉しきい値。0~100 の範囲で、パーセントで指定します。0 時の値は、自動チャネル調整がチャネル干渉しきい値を参照しないことを示します。

説明

チャネル干渉しきい値を設定するには、**interference-threshold** コマンドを使用します。

undo interference-threshold コマンドを使用して、デフォルトの状態を復元します。

チャネル干渉しきい値は、自動チャネル調整をトリガする条件の 1 つであり、AC は、すべてのデータフレームに対するチャネル内の干渉フレームの割合が設定値を超えたことを検出すると、チャネル調整をトリガする。干渉フレームは、現在動作している無線周波数以外のフレームです。

例

#チャネル干渉しきい値を 60 に設定します。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] interference-threshold 60

#チャネル干渉しきい値を 60 に設定します。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] interference-threshold 60

5.1.52 power holddown-time

Syntax

power holddown-time *minutes*

undo power holddown-time

デフォルト

パワーホールドアップ時間は 60 分です。

View

RRM holddown group view

定義済みユーザロール

network-admin

パラメータ

minutes:電力保持時間は、分単位で 10~1440 の値をとります。

説明

power holddown-time コマンドを使用して、待機電力を設定します。

undo power holddown-time コマンドを使用して、デフォルトの状態を復元します。

RRM ホールドアップチューニンググループに追加された RF 電力は、各調整後の電力ホールドアップ時間中は調整されません。

例

#RRM キープアライブグループ 10 の 600 分の電力キープアライブを設定します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10] power holddown-time 600

5.1.53 rrm

Syntax

rrm

デフォルト

RRM view が存在しません。

View

Radio view

定義済みユーザロール

network-admin

説明

rrm コマンドを実行すると、RRM (Radio Resource Management、無線リソース管理)view が表示されます。

例

#RRM view に移動します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

5.1.54 scan-only

Syntax

scan-only { **disable** | **enable** }

undo scan-only

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :無線周波数のスキャン機能がオフになっています。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

説明

scan-only enable コマンドは、無線周波数のスキャンを有効にします。

scan-only disable コマンドは、無線周波数のスキャン機能をオフにします。

undo scan-only コマンドを使用して、デフォルトの状態を復元します。

無線周波数のスキャン機能を起動した後、AP は無線環境に対してスキャンとデータ収集作業を行い、周期的にデータを AC に報告し、AC からチャネル報告と近隣報告を生成する。チャネルレポートとネイバーレポートの詳細は、display wlan rrm-status ap コマンドを使用して表示できます。

自動チャネル調整または自動電力調整を設定すると、無線周波数のスキャン機能が有効になります。したがって、自動チャネル調整または自動電力調整がすでに設定されている場合は、このコマンドを設定する必要はありません。

例

#無線周波数のチャネルスキャン機能を有効にします。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] scan-only enable

#無線周波数のチャネルスキャン機能を有効にします。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] scan-only enable

関連コマンド

- **display wlan rrm-status ap**

5.1.55 snmp-agent trap enable wlan rrm

Syntax

snmp-agent trap enable wlan rrm

undo snmp-agent trap enable wlan rrm

デフォルト

RRM アラーム機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan rrm コマンドを使用して、RRM アラーム機能を有効にします。

undo snmp-agent trap enable wlan rrm コマンドを使用して、RRM アラーム機能をオフにします。

RRM のアラーム機能をオンにすると、RF リソース管理によってアラーム情報が生成され、このモジュールの重要なイベントがネットワーク管理ソフトウェアに報告されます。この情報は SNMP モジュールに送信され、SNMP 内のアラーム情報の送信パラメータを設定することによって、アラーム情報の出力に関する属性を決定します。警告の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

例

#RRM のアラーム機能をオンにします。

<AC> system-view

[AC] snmp-agent trap enable wlan rrm

5.1.56 tolerance-level

Syntax

tolerance-level *percent*

undo tolerance-level

デフォルト

RRM view:AP グループの RRM 構成を継承します。

AP group's RRM view :グローバル構成を継承します。

View

RRM view

AP group's RRM view

定義済みユーザロール

network-admin

パラメータ

percent:許容係数。パーセントで表され、0~45 の値を取ります。0 は、チャネル調整計算が許容係数を参照しないことを示します。

説明

tolerance-level コマンドを使用して、許容係数を設定します。

undo tolerance-level コマンドを使用して、デフォルトの状態を復元します。

マージン係数は、チャネル調整前後の 2 チャネルのチャネル品質差分値である。

AC がチャネル品質の計算を開始すると、代替チャネル品質が現在のチャネルよりも優れており、許容係数に達するか、またはそれを超える場合にのみ、代替チャネルが適用される。

RRM view の許容範囲ファクタの構成は、AP グループの RRM view の構成よりも優先され、AP グループの RRM view の許容範囲ファクタの構成は、Global configuration view よりも優先されます。

例

#設定許容係数は 25 です。(RRM view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrm

[AC-wlan-ap-ap1-radio-1-rrm] tolerance-level 25

#設定許容係数は 25 です。(AP group's RRM view)

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] ap-model QX-W1020

[AC-wlan-ap-group-group1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1] rrm

[AC-wlan-ap-group-group1-ap-model-QX-W1020-radio-1-rrm] tolerance-level 25

5.1.57 wlan calibrate-channel pronto ap all

Syntax

ソフトウェアバージョン 9.4.09 を含む以降のソフトウェア

wlan calibrate-channel pronto ap { **all** | **ap-group** *group-name* } { **2.4g** | **5g** | **6g** | **all** }

ソフトウェアバージョン 9.4.05 のソフトウェア

wlan calibrate-channel pronto ap all

View

System view

定義済みユーザロール

network-admin

パラメータ

ソフトウェアバージョン 9.4.09 を含む以降のソフトウェア

ap all: 全ての AP を指定します。

ap-group *group-name*: 大文字と小文字を区別しない 1~31 文字で AP グループ名を指定します。

2.4g: 2.4GHz 無線を指定します。

5g: 5GHz 無線を指定します。

6g: 6GHz 無線を指定します。

all: 2.4GHz 無線と 5GHz 無線と 6GHz 無線のすべてを指定します。

ソフトウェアバージョン 9.4.05 のソフトウェア

指定できるパラメータはありません。

説明

wlan calibrate-channel pronto ap all コマンドは、自動チャネル調整のためにすべての AP の無線周波数を手動でトリガするために使用されます。

wlan calibrate-channel pronto ap all コマンドを実行すると、多くのシステムリソースを消費する可能性があるため、注意して使用してください。

例

#自動チャネル調整のためにすべての AP の無線周波数を手動でトリガします。

<AC> system-view

[AC] wlan calibrate-channel pronto ap all

5.1.58 wlan calibrate-power pronto ap all

Syntax

ソフトウェアバージョン 9.4.09 を含む以降のソフトウェア

wlan calibrate-power pronto ap { **all** | **ap-group** *group-name* } { **2.4g** | **5g** | **6g** | **all** }

ソフトウェアバージョン 9.4.05 のソフトウェア

wlan calibrate-power pronto ap all

View

System view

定義済みユーザロール

network-admin

パラメータ

ソフトウェアバージョン 9.4.09 を含む以降のソフトウェア

ap all: 全ての AP を指定します。

ap-group *group-name*: 大文字と小文字を区別しない 1~31 文字で AP グループ名を指定します。

2.4g: 2.4GHz 無線を指定します。

5g: 5GHz 無線を指定します。

6g: 6GHz 無線を指定します。

all: 2.4GHz 無線と 5GHz 無線と 6GHz 無線のすべてを指定します。

ソフトウェアバージョン 9.4.05 のソフトウェア

指定できるパラメータはありません。

説明

wlan calibrate-power pronto ap all コマンドは、自動電力調整のためにすべての AP の無線周波数を手動でトリガするために使用されます。

wlan calibrate-power pronto ap all コマンドを実行すると、多くのシステムリソースを消費する可能性があるため、注意して使用してください。

この機能は、最大送信電力が設定されている RF には適用されません。

例

#自動電力調整のためにすべての AP の無線周波数を手動でトリガします。

<AC> system-view

[AC] wlan calibrate-power pronto ap all

5.1.59 wlan rrm baseline apply

Syntax

wlan rrm baseline apply name *baseline-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name *baseline-name*:RF 動作パラメータのベースラインの名前。1~32 文字の文字列で、大文字と小文字は区別されません。

説明

wlan rrm baseline apply コマンドは、対応する無線周波数に無線周波数動作パラメータのベースラインを適用するために使用します。

無線周波数動作パラメータベースラインが次のいずれかに該当する場合、対応する無線周波数に無線周波数動作パラメータベースラインを適用することはできません。

- 無線周波数動作パラメータのベースラインには、現在のユーザが location 権限を持っていない AP の無線周波数情報が保存されます。
- RF 動作パラメータのベースラインは start_config_baseline.csv です。

例

#bl という名前の RF 動作パラメータのベースラインを適用します。

<AC> system-view

[AC] wlan rrm baseline apply name bl

関連コマンド

- **display wlan rrm baseline apply-history**
- **wlan rrm baseline save**

5.1.60 wlan rrm baseline remove

Syntax

wlan rrm baseline remove name *baseline-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name *baseline-name*:RF 動作パラメータのベースラインの名前。1~32 文字の文字列で、大文字と小文字は区別されません。

説明

wlan rrm baseline remove コマンドを使用して、RF 動作パラメータのベースラインを削除します。

無線周波数動作パラメータのベースラインに、現在のユーザが location 権限を持っていない AP の無線周波数情報が保存されている場合、そのユーザは無線周波数動作パラメータのベースラインを削除できません。

例

#bl という名前の RF 動作パラメータのベースラインを削除します。

<AC> system-view

[AC] wlan rrm baseline remove name bl

関連コマンド

- **wlan rrm baseline save**

5.1.61 wlan rrm baseline save

Syntax

wlan rrm baseline save name *baseline-name* { **ap** *ap-name* [**radio** *radio-id*] | **ap-group** *group-name* [**ap-model** *ap-model*] [**radio** *radio-id*] | **global** }

View

System view

定義済みユーザロール

network-admin

パラメータ

name *baseline-name*:RF 動作パラメータのベースラインの名前。1~32 文字の文字列で、大文字と小文字は区別されません。

ap *ap-name*:AP の名前。1~64 文字の文字列で、英数字、アンダースコア、.、[」 、 「]、/、-を使用できます。大文字と小文字は区別されます。このパラメータを指定する場合、AP はすでに存在している必要があります。

radio *radio-id*:AP 無線周波数の番号。このパラメータが指定されていない場合、指定されたモデルの AP/AP グループ/AP グループのすべての無線周波数の動作パラメータが保存されます。

ap-group *group-name*:AP グループの名前。1~31 文字の文字列で、大文字と小文字は区別されません。このパラメータを指定する場合、AP グループはすでに存在している必要があります。

ap-model *ap-model*:AP モデル名。このパラメータを指定しない場合、AP グループで指定された、またはすべての無線周波数の動作パラメータが保存されます。

global:AC 上のすべての無線。

説明

wlan rrm baseline save コマンドは、現在の無線周波数の動作パラメータを動作パラメータのベースラインとして保存します。

現在の無線周波数の動作チャネルおよび電力値が適切である場合、このコマンドを使用して、無線周波数のチャネルおよび電力値を無線周波数動作パラメータのベースラインとして格納し、必要に応じてこれらの格納された値を再適用することができる。

RF 動作パラメータのベースラインは、.csv ファイルとしてファイルシステムに保存されます。

例

#AP 1 の Radio 1 の動作パラメータを、無線周波数動作パラメータのベースラインとして ap1-1 という名前で保存します。

<AC> system-view

[AC] wlan rrm baseline save name ap1-1 ap ap1 radio 1

#AP 1 の AP group's Radio 1 の動作パラメータを、無線周波数動作パラメータのベースラインとして ap1g1-1 という名前で保存します。

<AC> system-view

[AC] wlan rrm baseline save name ap1g1-1 ap-group group1 ap-model QX-W1020 radio 1

#AC 上のすべての RF の動作パラメータを、global という名前の RF 動作パラメータのベースラインとして保存します。

<AC> system-view

[AC] wlan rrm baseline save name global global

5.1.62 wlan rrm calibration-bandwidth interval

Syntax

wlan rrm calibration-bandwidth interval *minutes*

undo wlan rrm calibration-bandwidth interval

デフォルト

自動帯域幅調整周期は 13 分。

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes:分単位で 3~1440 の範囲の自動帯域幅調整サイクル。

説明

wlan rrm calibration-bandwidth interval コマンドを使用して、自動帯域幅調整サイクルを設定します。

undo wlan rrm calibration-bandwidth interval コマンドを使用して、デフォルトの状態を復元します。

例

#自動帯域幅調整サイクルを 10 分に設定します。

<AC> system-view

[AC] wlan rrm calibration-bandwidth interval 10

関連コマンド

- **calibrate-bandwidth self-decisive**

5.1.63 wlan rrm calibration-channel interval

Syntax

wlan rrm calibration-channel interval *minutes*

undo wlan rrm calibration-channel interval

デフォルト

自動チャネル調整期間は 23 分。

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes:自動チャネル調整周期は、 3~1440 の範囲で、単位は分である。

説明

wlan rrm calibration-channel interval コマンドを使用して、自動チャネル調整サイクルを設定します。

undo wlan rrm calibration-channel interval コマンドを使用して、デフォルトの状態を復元します。

例

#自動チャネル調整期間を 10 分に設定します。

<AC> system-view

[AC] wlan rrm calibration-channel interval 10

関連コマンド

- **calibrate-channel self-decisive**

5.1.64 wlan rrm calibration-power interval

Syntax

wlan rrm calibration-power interval *minutes*

undo wlan rrm calibration-power interval

デフォルト

自動電力調整サイクルは 11 分。

View

System view

定義済みユーザロール

network-admin

パラメータ

minutes:分単位で 3~180 の範囲の自動電力調整サイクル。

説明

wlan rrm calibration-power interval コマンドを使用して、自動電力調整サイクルを設定します。

undo wlan rrm calibration-power interval コマンドを使用して、デフォルトの状態を復元します。

例

#自動電源調整サイクルを 10 分に設定します。

<AC> system-view

[AC] wlan rrm calibration-power interval 10

関連コマンド

- **calibrate-power self-decisive**

5.1.65 wlan rrm-calibration-group

Syntax

wlan rrm-calibration-group *group-id*

undo wlan rrm-calibration-group { **all** | *group-id* }

デフォルト

RRM 保持調整グループがありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

all:すべての RRM は調整グループを保持します。

group-id:RRM は調整グループの ID を 1~128 の範囲の値で保持します。

説明

wlan rrm-calibration-group コマンドは、RRM ホールドダウングループを作成し、そのビューを入力するか、既存の RRM ホールドダウングループのビューを入力します。

undo wlan rrm-calibration-group コマンドを使用して、作成した RRM ホールドアップグループを削除します。

例

#ID 10 の RRM キープアライブグループを作成します。

<AC> system-view

[AC] wlan rrm-calibration-group 10

[AC-wlan-rrm-calibration-group-10]

5.1.66 wlan rrm high-density filter

🕮 **メモ：**

このコマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

wlan rrm high-density filter { **all** | **ap-group** *group-name* } { **2.4g** | **5g** | **6g** | **all** }

View

System view

定義済みユーザロール

network-admin

パラメータ

all:すべての AP を指定します。

ap-group *group-name*:大文字と小文字は区別しない 1～31 文字で AP グループ名を指定します。

2.4g:2.4GHz 無線を指定します。

5g: 5GHz 無線を指定します。

6g: 6GHz 無線を指定します。

all: 全ての無線を指定します。

説明

wlan rrm high-density filter コマンドは、高密度シナリオでシャットダウンできる AP を除外します。

高密度シナリオでは、チャネルリソースが限られているため、隣接 AP 間で AP 間干渉が避けられない場合があります。密度が高いほど、干渉が大きくなります。

高密度シナリオでチャネル調整によって干渉を削減できない場合は、このタスクを実行して、シャットダウンできる AP をフィルタで除外できます。フィルタ処理後、**display wlan rrm high-density filter history** コマンドを実行して、フィルタで除外した AP を表示し、手動で AP を無効にします。

例

AP グループ group1 でシャットダウンできる 5 GHz 無線をフィルタで除外します。

<AC> system-view

[AC] wlan rrm high-density filter ap-group group1 5g

すべての AP 間でシャットダウンできるすべての無線を除外する。

<AC> system-view

[AC] wlan rrm high-density filter all all

目次

このセクションのページは **9-x-x** です。

6 章 バンドナビゲーション 6-1
6.1 バンドナビゲーション設定コマンド 6-1
6.1.1 band-navigation 6-1
6.1.2 wlan band-navigation aging-time 6-2
6.1.3 wlan band-navigation balance access-denial 6-3
6.1.4 wlan band-navigation balance session 6-3
6.1.5 wlan band-navigation enable 6-4
6.1.6 wlan band-navigation rssi-threshold 6-5

6章 バンドナビゲーション

6.1 バンドナビゲーション設定コマンド

6.1.1 band-navigation

Syntax

band-navigation { **disable** | **enable** }

undo band-navigation

デフォルト

APView では、AP は AP group View の設定を使用します。

AP group View では、AP グループに対してバンドナビゲーションが有効になっています。

View

AP View

AP group View

定義済みユーザロール

network-admin

説明

band-navigation enable コマンドで、 AP または AP グループのバンドナビゲーションを有効にします。

band-navigation disable コマンドで、 AP または AP グループのバンドナビゲーションを無効にします。

undo band-navigation コマンドで、デフォルトに戻ります。

バンドナビゲーションは、グローバルと AP の両方でバンドナビゲーションを有効にした後でのみ AP で有効になります。

例

#AP ap1 のバンドナビゲーションを有効にする。

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] band-navigation enable

#AP グループ 1 のバンドナビゲーションを有効にする。

<Sysname> system-view

[Sysname] wlan ap-group 1

[Sysname-wlan-ap-group-1] band-navigation enable

関連コマンド

- wlan band-navigation enable

6.1.2 wlan band-navigation aging-time

Syntax

wlan band-navigation aging-time *aging-time*

undo wlan band-navigation aging-time

デフォルト

180 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time： クライアント情報のエージングタイムを 10～600 秒の範囲で指定します。

説明

wlan band-navigation aging-time コマンドで、クライアント情報のエージングタイムを設定します。

undo wlan band-navigation aging-time コマンドで、デフォルトに戻します。

AP がクライアントからアソシエーション要求を受信すると、AP はクライアントの情報を記録し、クライアント情報のエージングタイマを開始します。エージングタイマの期限が切れる前に AP がクライアントからプローブ要求またはアソシエーション要求を受信した場合、AP はクライアント情報を更新し、エージングタイマのクライアント情報をリセットします。エージングタイマの期限が切れる前に、AP がクライアントからプローブ要求またはアソシエーション要求を受信しない場合、AP はクライアントの情報を削除します。

クライアントアソシエーションとシステムリソースの両方の効率性を確保するために、適切なクライアント情報のエージングタイムを設定します。

例

#クライアント情報のエージングタイムを 50 秒に設定する。

<Sysname> system-view

[Sysname] wlan band-navigation aging-time 50

6.1.3 wlan band-navigation balance access-denial

Syntax

wlan band-navigation balance access-denial *access-denial*

undo wlan band-navigation balance access-denial

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

access-denial : 5 GHz アソシエーション要求に対する拒否の最大数を 1～10 の範囲で指定します。

説明

wlan band-navigation balance access-denial コマンドで、5GHz アソシエーション要求に対する拒否の最大数を設定します。

undo wlan band-navigation balance access-denial コマンドで、デフォルトに戻します。

5GHz 無線がクライアントを拒否する回数が指定された最大数に達すると、無線はクライアントのアソシエーション要求を受け入れます。

例

#5 GHz アソシエーション要求に対する拒否の最大数を 5 に設定します。

<Sysname> system-view

[Sysname] wlan band-navigation balance access-denial 5

6.1.4 wlan band-navigation balance session

Syntax

wlan band-navigation balance session *session* [**gap** *gap*]

undo wlan band-navigation balance session

デフォルト

ロードバランシングはバンドナビゲーションに対して無効になっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

session ： 5GHz 無線のクライアント番号のしきい値を 2～255 の範囲で指定します。

gap ： 5GHz 無線とクライアントが最も少ない無線との間のクライアント番号ギャップのしきい値を指定します。この引数の値の範囲は 1~8 で、デフォルト値は 4 です。

説明

wlan band-navigation balance session コマンドで、バンドナビゲーションのロードバランシングを設定します。

undo wlan band-navigation balance session コマンドで、デフォルトに戻します。

バンドナビゲーションを有効にしてもロードバランシングを有効にしない場合、AC はデュアルバンドクライアントを 5GHz 無線に誘導します。

次の条件が満たされている場合、AP はクライアントの 5GHz アソシエーション要求を拒否します。

- 5GHz 無線のクライアント数が指定したしきい値に達しました。
- 5GHz 無線とクライアントが最も少ない無線との間のクライアント番号のギャップが、指定されたしきい値に達します。

例

#バンドナビゲーションのロードバランシングを有効にし、クライアント番号のしきい値とセッションギャップのしきい値をそれぞれ 10 と 5 に設定する。

<Sysname> system-view

[Sysname] wlan band-navigation balance session 10 gap 5

6.1.5 wlan band-navigation enable

Syntax

wlan band-navigation enable

undo wlan band-navigation enable

デフォルト

バンドナビゲーションはグローバルに無効になっています。

View

System view

定義済みユーザロール

network-admin

説明

wlan band-navigation enable コマンドで、バンドナビゲーションをグローバルに有効にします。

undo wlan band-navigation enable コマンドで、デフォルトに戻します。

バンドナビゲーションを有効にするには、クライアントが使用するワイヤレスサービスの高速アソシエーションが無効になっていることを確認します。

バンドナビゲーションは、グローバルと AP の両方でバンドナビゲーションを有効にした場合にのみ AP で有効になります。

例

#バンドナビゲーションをグローバルに有効にする。

<Sysname> system-view

[Sysname] wlan band-navigation enable

関連コマンド

- band-navigation
- quick-association enable

6.1.6 wlan band-navigation rssi-threshold

Syntax

wlan band-navigation rssi-threshold *rssi-threshold*

undo wlan band-navigation rssi-threshold

デフォルト

15

View

System view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold：バンドナビゲーションの RSSI しきい値を 5～100 の範囲で指定します。

説明

wlan band-navigation rssi-threshold コマンドで、バンドナビゲーションの受信信号強度インジケータ (RSSI) のしきい値を設定します。

undo wlan band-navigation rssi-threshold コマンドで、デフォルトに戻します。

クライアントが複数の無線によって検出される場合があります。5GHz 無線は、クライアントの RSSI がバンドナビゲーション RSSI しきい値より低い場合、クライアントのアソシエーション要求を拒否します。

例

#バンドナビゲーションの RSSI しきい値を 40 に設定する。

<Sysname> system-view

[Sysname] wlan band-navigation rssi-threshold 40

目次

このセクションのページは **9-x-x** です。

7 章 チャネルスキャン 7-1
7.1 チャネルスキャン設定コマンド 7-1
7.1.1 scan channel blacklist 7-1
7.1.2 scan channel whitelist 7-2
7.1.3 scan idle-time 7-3
7.1.4 scan max-service-time 7-4
7.1.5 scan scan-time 7-6
7.1.6 wlan channel-report disable 7-7
7.1.7 wlan channel-report interval 7-8
7.1.8 wlan neighbor-report disable 7-8
7.1.9 wlan neighbor-report interval 7-9

7章 チャネルスキャン

7.1 チャネルスキャン設定コマンド

7.1.1 scan channel blacklist

Syntax

scan channel blacklist *channel-list*

undo scan channel blacklist { *channel-list* | **all** }

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group's radio view で、チャネルスキャンのブラックリストが設定されていません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

channel-list:国別コードと無線周波数モードによって決定されるチャネルリスト。

all:チャネルスキャンブラックリストからすべてのチャネルを削除することを示します。

説明

チャネルスキャンブラックリストを設定するには、**scan channel blacklist** コマンドを使用します。

undo scan channel blacklist コマンドは、設定されたチャネルスキャンのブラックリストを削除するために使用されます。

チャネルスキャンのブラックリストが設定されている場合、AP はブラックリストに含まれている非動作チャネルをスキャンしません。チャネルスキャンのホワイトリストとブラックリストを同時に設定することはできません。

AP view の設定は、AP group’s view の設定よりも優先されます。

例

#チャネル 1、6 をチャネルスキャンのブラックリストに追加します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap 1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 2

[Sysname-wlan-ap-ap1-radio-2] scan channel blacklist 1 6

#チャネル 1、6 をチャネルスキャンのブラックリストに追加します。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group 10

[Sysname-wlan-ap-group-10] ap-model QX-W1020

[Sysname-wlan-ap-group-10-ap-model-QX-W1020] radio 2

[Sysname-wlan-ap-group-10-ap-model-QX-W1020-radio-2] scan channel blacklist 1 6

7.1.2 scan channel whitelist

Syntax

scan channel whitelist *channel-list*

undo scan channel whitelist { *channel-list* | **all** }

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group's radio view で、チャネルスキャンリストのホワイトリストリストが設定されていません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

channel-list:国別コードと無線周波数モードによって決定されるチャネルリスト。

all:チャネルスキャンのホワイトリストからすべてのチャネルを削除することを示します。

説明

チャネルスキャンのホワイトリストリストを設定するには、**scan channel whitelist** コマンドを使用します。

undo scan channel whitelist コマンドは、設定されたチャネルスキャンのホワイトリストを削除するために使用されます。

チャネルスキャンのホワイトリストを設定すると、AP は、動作中のチャネルとホワイトリストに存在する非動作中のチャネルのみをスキャンします。チャネルスキャンのホワイトリストとブラックリストを同時に設定することはできません。

AP view の設定は、AP group’s view の設定よりも優先されます。

例

#チャネル 1、6 をチャネルスキャンのホワイトリストに追加します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap 1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 2

[Sysname-wlan-ap-ap1-radio-2] scan channel whitelist 1 6

#チャネル 1、6 をチャネルスキャンのホワイトリストに追加します。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group 10

[Sysname-wlan-ap-group-10] ap-model QX-W1020

[Sysname-wlan-ap-group-10-ap-model-QX-W1020] radio 2

[Sysname-wlan-ap-group-10-ap-model-QX-W1020-radio-2] scan channel whitelist 1 6

7.1.3 scan idle-time

Syntax

scan idle-time *idle-time*

undo scan idle-time

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group's radio view の下で、サービスサイクルアイドル時間は 100 ミリ秒です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

idle-time:60~5000 ミリ秒の値を持つ、サービスサイクルのアイドル時間。

説明

scan idle-time コマンドを使用して、サービスサイクルのアイドル時間を設定します。

undo scan idle-time コマンドを使用して、デフォルトの状態を復元します。

サービスサイクルアイドル時間は、サービスサイクル中にワークチャネルでトラフィックがない状態が続く時間です。

1 つのサービスサイクルで、トラフィックのない期間がアイドル時間に達し、現在のサイクルが 1 スキャンサイクル時間を超えて停止した場合、次のスキャンサイクルに切り替えます。スキャン時間に達していない場合は、アイドル時間が経過してもスキャンサイクルに切り替わりません。サービスサイクルのアイドル時間とスキャン時間のどちらも、サービスサイクルの最大時間を超えることはできません。

scan idle-time は、設定された idle-time が beacon interval より小さい場合に、beacon interval の整数倍の時間に実際に有効に beacon interval なります。

AP view の設定は、AP group’s view の設定よりも優先されます。

例

#サービスサイクルのアイドル時間を 500 ミリ秒に設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] scan idle-time 500

#サービスサイクルのアイドル時間を 500 ミリ秒に設定します。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group 10

[Sysname-wlan-ap-group-10] ap-model QX-W1020

[Sysname-wlan-ap-group-10-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-10-ap-model-QX-W1020-radio-1] scan idle-time 500

関連コマンド

- **beacon interval**

7.1.4 scan max-service-time

Syntax

scan max-service-time { *max-service-time* | **no-limit** }

undo scan max-service-time

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group's radio view では、サービスサイクルの最大期間は 5000 ミリ秒です。

View

Radio view

AP group’s radio view

定義済みユーザロール

network-admin

パラメータ

max-service-time:100~5000 ミリ秒の範囲の値を持つ、サービスサイクルの最大継続時間。

no-limit:チャネルがアイドル状態になるまで(ワークチャネルのトラフィックがない状態が続く期間が、サービスサイクルのアイドル時間に達する)、スキャンサイクルに切り替わるまで、サービスサイクルの最大継続時間は制限されません。サービスサイクルの最大期間が no-limit に設定されている場合、AP は常にサービスクラストラフィックを優先し、トラフィックが存在する限りスキャンしません。

説明

scan max-service-time コマンドを使用して、サービスサイクルの最大期間を設定します。

undo scan max-service-time コマンドを使用して、デフォルトの状態を復元します。

現在のサービスサイクルが最大期間に達すると、トラフィックが停止しているかどうかにかかわらず、次のスキャンサイクルに切り替わります。サービスサイクルの最大期間は、スキャンサイクルの期間より短くすることはできません。

AP view の設定は、AP group’s view の設定よりも優先されます。

例

#サービスサイクルの最大期間を 3000 ミリ秒に設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] scan max-service-time 3000

#サービスサイクルの最大期間を 3000 ミリ秒に設定します。(AP group’s radio view)

<Sysname> system-view

[Sysname] wlan ap-group 10

[Sysname-wlan-ap-group-10] ap-model QX-W1020

[Sysname-wlan-ap-group-10-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-10-ap-model-QX-W1020-radio-1] scan max-service-time 3000

7.1.5 scan scan-time

Syntax

scan scan-time *scan-time*

undo scan scan-time

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group’s radio view でのスキャン時間は 100 ミリ秒です。

View

Radio view

AP group’s radio view

定義済みユーザロール

network-admin

パラメータ

scan-time:スキャン時間をミリ秒単位で 100~5000 の範囲で指定します。

説明

scan scan-time コマンドを使用して、スキャン時間を設定します。

undo scan scan-time コマンドを使用して、デフォルトの状態を復元します。

スキャン時間とは、無線周波数チャネルのスキャン時間の長さを指し、同時にサービス期間内にスキャンを提供する時間の長さを規定することにも用いられ、スキャン時間の長さはサービス期間の最大持続時間を超えてはならない。現在のスキャンサイクルがスキャン時間に達すると、次のスキャンサイクルまたはサービスサイクルに切り替わります。

AP view の設定は、AP group’s view の設定よりも優先されます。

例

#スキャン時間を 500 ミリ秒に設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] scan scan-time 500

#スキャン時間を 500 ミリ秒に設定します。(AP group’s radio view)

<Sysname> system-view

[Sysname] wlan ap-group 10

[Sysname-wlan-ap-group-10] ap-model QX-W1020

[Sysname-wlan-ap-group-10-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-10-ap-model-QX-W1020-radio-1] scan scan-time 500

7.1.6 wlan channel-report disable

Syntax

wlan channel-report disable

undo wlan channel-report disable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan channel-report disable コマンドを使用して、AP によるチャネルレポートの送信を無効にします。

undo wlan channel-report disable を使用して、AP によるチャネルレポートの送信を有効にします。

チャネルレポートには、チャネル負荷、チャネル使用率、チャネル干渉、ビットエラー率、再送信率などのチャネル情報が含まれます。

チャネルレポート送信が無効になっている場合、自動チャネル調整、自動電力調整、および無線リソース測定は使用できません。

例

#AP によるチャネルレポートの送信を無効にします。

<Sysname> system-view

[Sysname] wlan channel-report disable

関連コマンド

- **calibrate-channel self-decisive(無線管理/WLAN RRM)**

7.1.7 wlan channel-report interval

Syntax

wlan channel-report interval *interval*

undo wlan channel-report interval

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:AP がチャネルレポートを送信する間隔を 50~86400 秒の範囲で指定します。

説明

wlan channel-report interval コマンドを使用して、AP がチャネルレポートを送信する間隔を設定します。

undo wlan channel-report interval コマンドを使用して、デフォルトに戻します。

適切なレポート間隔を設定します。レポート間隔が小さいと、AC 負荷が高くなります。レポート間隔が大きいと、自動チャネル調整と自動電源調整に影響します。

例

#AP がチャネルレポートを送信する間隔を 1800 秒に設定します。

<Sysname> system-view

[Sysname] wlan channel-report interval 1800

関連コマンド

- **wlan rrm calibration-channel interval (無線管理/WLAN RRM)**

7.1.8 wlan neighbor-report disable

Syntax

wlan neighbor-report disable

undo wlan neighbor-report disable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan neighbor-report disable コマンドを使用して、AP による近隣レポートの送信を無効にします。

undo wlan neighbor-report disable コマンドを使用して、AP による近隣レポートの送信を有効にします。

ネイバーレポートには、RSSI などのネイバー無線情報が含まれます。

ネイバーレポート送信が無効になっている場合、自動チャネル調整、自動電力調整、および無線リソース測定は使用できません。

例

#AP による近隣レポートの送信を無効にします。

<Sysname> system-view

[Sysname] wlan neighbor-report disable

関連コマンド

- **calibrate-channel self-decisive (無線管理/WLAN RRM)**

7.1.9 wlan neighbor-report interval

Syntax

wlan neighbor-report interval *interval*

undo wlan neighbor-report interval

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

説明

wlan neighbor-report interval コマンドを使用して、AP が近隣レポートを送信する間隔を設定します。

undo wlan neighbor-report interval コマンドを使用します。デフォルトに戻します。

適切なレポート間隔を設定します。レポート間隔が小さいと、AC 負荷が高くなります。レポート間隔が大きいと、自動チャネル調整と自動電源調整に影響します。

例

#AP が近隣レポートを送信する間隔を 1800 秒に設定します。

<Sysname> system-view

[Sysname] wlan neighbor-report interval 1800

関連コマンド

- **wlan rrm calibration-channel interval (無線管理/WLAN RRM)**

目次

このセクションのページは **9-x-x** です。

8 章 スペクトル管理 8-1
8.1 スペクトル管理設定コマンド 8-1
8.1.1 channel-capability mode 8-1
8.1.2 channel-switch mode 8-2
8.1.3 power-capability mode 8-4
8.1.4 power-constraint mode 8-5
8.1.5 spectrum-management 8-7

8章 スペクトル管理

8.1 スペクトル管理設定コマンド

8.1.1 channel-capability mode

Syntax

channel-capability mode { **all** | **none** | **partial** }

undo channel-capability mode

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group's radio view の下で、クライアントチャネル機能セットをチェックしません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

all:完全一致パターン。クライアントがオンラインになるのは、クライアントのチャネル機能セットが Radio のチャネル機能セットとすべて一致する場合のみです。一致しない場合、クライアントはオンラインになりません。

none:モードをチェックしません。つまり、クライアントのチャネル機能セットをチェックしません。

partial:部分一致パターン。クライアントのチャネルコンピテンシーセットと Radio のチャネルコンピテンシーセットが交差している場合、クライアントはオンラインになります。交差していない場合、クライアントはオンラインになりません。

説明

🕮 **メモ** :

このコマンドは、5 GHz 無線でのみサポートされています。

クライアントチャネル機能セットの検査モードを設定するには、channel-capability mode コマンドを使用します。

undo channel-capability mode コマンドを使用して、デフォルトの状態を復元します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#クライアントチャネル機能セットのチェックモードを完全一致モードに設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] spectrum-management enable

[Sysname-wlan-ap-ap1-radio-1] channel-capability mode all

#クライアントチャネル機能セットのチェックモードを完全一致モードに設定します。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel-capability mode all

関連コマンド

- **spectrum-management**

8.1.2 channel-switch mode

Syntax

channel-switch mode { **continuous** | **suspend** }

undo channel-switch mode

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group's radio view では、アップリンクされたクライアントはチャネル切り替え中にフレームの送信を停止します。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

continuous:アップリンクされたクライアントは、チャネルの切り替え中にフレームを送信し続けることができます。

suspend:チャネルの切り替え中、アップリンクされたクライアントは、チャネルの切り替えが完了するまでフレームの送信を停止します。

説明

チャネル切り替えモードを設定するには、**channel-switch mode** コマンドを使用します。

undo channel-switch mode コマンドを使用して、デフォルトの状態を復元します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#設定チャネルが切り替わる間、アップリンクされたクライアントはフレームを送信し続けることができます。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] spectrum-management enable

[Sysname-wlan-ap-ap1-radio-1] channel-switch mode continuous

#設定チャネルが切り替わる間、アップリンクされたクライアントはフレームを送信し続けることができます。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] channel-switch mode continuous

関連コマンド

- **spectrum-management**

8.1.3 power-capability mode

Syntax

power-capability mode { **all** | **none** | **partial** }

undo power-capability mode

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group's radio view の下で、クライアント電力能力セットをチェックしません。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

all:完全一致パターン。クライアントがオンラインになるのは、クライアントの電力能力セットが Radio の電力能力セットとすべて一致する場合のみです。それ以外の場合は、クライアントはオンラインになりません。

none:モードをチェックしません。つまり、クライアントの電力能力セットをチェックしません。

partial:部分一致パターン。クライアントの Power Capability Set が Radio の Power Capability Set と一致する場合、クライアントはオンラインになります。一致しない場合、クライアントはオンラインになりません。

説明

power-capability mode コマンドを使用して、クライアントの電力能力セットの検査モードを設定します。

undo power-capability mode コマンドを使用して、デフォルトの状態を復元します。

スペクトラム管理機能または RF リソース測定機能がオンになっている場合にのみ、電力能力セットチェック機能が有効になります。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#クライアントの電力能力セットのチェックモードを完全一致モードに設定します。
(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] spectrum-management enable

[Sysname-wlan-ap-ap1-radio-1] power-capability mode all

#クライアントの電力能力セットのチェックモードを完全一致モードに設定します。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] power-capability mode all

関連コマンド

- **resource-measure**
- **spectrum-management**

8.1.4 power-constraint mode

Syntax

power-constraint mode { **auto** [**anpi-interval** *anpi-interval-value*] | **manual** *power-constraint* }

undo power-constraint mode

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group's radio view では、電力制限モードは自動モードです。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

auto:自動モード。

anpi-interval *anpi-interval-value*:ANPI (Average Noise Power Indicator、平均雑音電力識別)の差を dBm 単位で 0~30 の範囲で指定します。デフォルト値は 10 です。

manual power-constraint:手動モードでの電力制限値は、0～30 の範囲で、単位は dBm。

説明

🕮 **メモ** ：

このコマンドは、5 GHz 無線でのみサポートされています。

power-constraint mode コマンドを使用して、電力制限モードを設定します。

undo power-constraint mode コマンドを使用して、デフォルトの状態を復元します。

自動モードに設定すると、デバイスは、受信チャネル電力パラメータ、平均ノイズフロア電力、ANPI 差に基づいて制限電力値を計算します。計算式:power-constraint =RCPI (Received Channel Power Indicator、受信チャネル電力 ID)-(ANPI+anpi-interval-value)。

電力制限機能は、スペクトル管理機能または無線周波数リソース測定機能がオンになっている場合にのみ有効です。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#設定 5 GHz モードのクライアントの電力制限モードは手動モードで、電力制限値は 5 dBm です。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] spectrum-management enable

[Sysname-wlan-ap-ap1-radio-1] power-constraint mode manual 5

#設定 5 GHz モードのクライアントの電力制限モードは手動モードで、電力制限値は 5 dBm です。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] power-constraint mode manual 5

関連コマンド

- **resource-measure**
- **spectrum-management**

8.1.5 spectrum-management

Syntax

spectrum-management { **disable** | **enable** }

undo spectrum-management

デフォルト

Radio view の下で、AP グループ Radio 設定を引き継ぎます。

AP group's radio view で、スペクトル管理機能がオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

🕮 メモ ：

このコマンドは、5 GHz 無線でのみサポートされています。

spectrum-management enable コマンドを使用して、スペクトル管理機能を有効にします。

spectrum-management disable コマンドを使用して、スペクトル管理機能をオフにします。

undo spectrum-management コマンドを使用して、デフォルトの状態を復元します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#スペクトル管理機能をオンにします。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] spectrum-management enable

#スペクトル管理機能をオンにします。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1020

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1020-radio-1] spectrum-management enable

QX-W2300AC シリーズアクセスコントローラ

コマンドマニュアル

10.WLAN ローミング

本マニュアルは以下に示す章で構成されています。

01-WLAN ローミング

02-拡張ローミング

03-モビリティグループ

目次

このセクションのページは **10-x-x** です。

1 章 WLAN ローミング 1-1
1.1 WLAN ローミング設定コマンド 1-1
1.1.1 client cache aging-time 1-1
1.1.2 display wlan mobility roam-track mac-address 1-2

1章 WLAN ローミング

1.1 WLANローミング設定コマンド

1.1.1 client cache aging-time

Syntax

client cache aging-time *aging-time*

undo client cache aging-time

デフォルト

ワイヤレスクライアントのローミングテーブルエントリのエージングタイムは 180 秒です。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

aging-time:無線クライアント Cache のエージングタイム。0~86400 の範囲で秒単位で指定します。

説明

クライアントローミングテーブルエントリのエージングタイムを設定するには、**client cache aging-time** コマンドを使用します。

undo client cache aging-time コマンドを使用して、デフォルトの状態を復元します。

ワイヤレスクライアントのローミングテーブルエントリのエージングタイムを 0 時に設定すると、クライアントのローミングテーブルエントリに関する情報は、クライアントがオフラインになった直後に削除されます。

このコマンドは、ワイヤレスサービステンプレートがオフの場合にのみ設定できます。

例

#クライアントローミングテーブルエントリのエージングタイムを 100 秒に設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] client cache aging-time 100

1.1.2 display wlan mobility roam-track mac-address

Syntax

display wlan mobility roam-track mac-address *mac-address*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*:クライアントを MAC アドレスで H-H-H の形式で指定します。

説明

display wlan mobility roam-track mac-address コマンドを使用して、クライアントのローミング情報を表示します。

ローミング情報が順番に表示されます。最新のロームトラック情報が最初に表示されます。

システムは、最大 128 個のローミングトラックエントリを保存できます。最大数に達したときに新しいローミングエントリを追加するには、システムは 126 番目のエントリを削除してから、新しいエントリを追加します。

例

#指定したクライアントのローミング情報をホーム AC に表示します。

<Sysname> display wlan mobility roam-track mac-address 5250-0012-0411

Total entries: 2

```
BSSID         Created at          Online time      AC IP address  RID  AP name
3ce5-a68d-2280  2016-06-14 11:12:28  00hr 48min 46sec  127.0.0.1     2    ap1
0026-3e08-1150  2016-06-14 11:12:05  00hr 40min 46sec  127.0.0.1     2    ap2
```

表 1-1 display wlan mobility roam-track mac-address コマンドの表示情報の説明

フィールド	説明
BSSID	クライアントが関連付けられているAPのBSSID
Created at	クライアントのロームトラックエントリが作成された時刻
Online time	クライアントのオンライン時刻

フィールド	説明
AC IP address	クライアントが関連付けられているACのIPアドレス。このフィールドには127.0.0.1が表示されます
RID	クライアントが関連付けられている無線のID
AP name	クライアントが関連付けられているAPの名前

目次

このセクションのページは **10-x-x** です。

2 章 拡張ローミング 2-1
2.1 拡張ローミング設定コマンド 2-1
2.1.1 bss transition-management enable 2-1
2.1.2 bss transition-management disassociation 2-2
2.1.3 ft enable 2-3
2.1.4 ft mobility-domain-id 2-4
2.1.5 ft reassociation-timeout 2-5
2.1.6 mac-authentication fast-connect enable 2-6
2.1.7 sacp anti-sticky 2-7

2章 拡張ローミング

2.1 拡張ローミング設定コマンド

2.1.1 bss transition-management enable

Syntax

bss transition-management enable

undo bss transition-management enable

デフォルト

BSS スイッチオーバー管理機能がオフになっています。

View

Service template view

定義済みユーザロール

network-admin

説明

bss transition-management enable コマンドは、BSS スイッチ管理機能を有効にします。

undo bss transition-management enable コマンドは、BSS スイッチオーバー管理機能をオフにします。

BSS 切換管理機能を起動した後、設備はある無線クライアントの信号強度が閾値より低いことを検出して、或は無線クライアントが発行する切換問い合わせ要求メッセージを受信すると、無線クライアントに BSS 切換を要求する通知を送信して、無線クライアントを他の BSS に接続するように誘導する。無線クライアントは、 BSS 切替え要求通知を受信すると、 BSS 切替えの動作を行うかどうかを自律的に決定する。

ワイヤレスクライアントの anti-sticky 機能がオフの場合、デバイスは、ワイヤレスクライアントの信号強度がしきい値を下回っているかどうかを検出しません。

このコマンドは、ワイヤレスサービステンプレートがオフの場合にのみ設定できます。

BSS スイッチオーバー管理を有効にし、bss transition-management disassociation コマンドを使用して BSS スイッチオーバーの関連付け解除時間を設定することをお勧めします。設定しないと、一部のクライアントで BSS スイッチオーバーが失敗する可能性があります。

例

#BSS スイッチ管理機能をオンにします。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] bss transition-management enable

関連コマンド

- **bss transition-management disassociation**
- **sacp anti-sticky**

2.1.2 bss transition-management disassociation

Syntax

bss transition-management disassociation { **forced** | **recommended** } [**timer** *time*]

undo bss transition-management disassociation

デフォルト

BSS カットオーバーアソシエーション解除機能がオンの場合、デバイスはクライアントに BSS カットオーバーを推奨します。アソシエーション解除推奨時間は 90 秒です。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

forced:クライアントに BSS スイッチオーバーを強制します。つまり、BSS スイッチオーバーの関連付けが解除されてから時間が経過してもクライアントが移動しない場合、デバイスはクライアントからの接続を強制的に切断します。

recommended:クライアントは、BSS スイッチオーバーを実行することを推奨します。これは、BSS スイッチオーバーのアソシエーション解除時間が経過してもクライアントが移動しない場合、デバイスがクライアントからの接続を強制的に切断しないことを意味します。

timer *time*:BSS スイッチで強制的に(または推奨)関連付けを解除するには、0~180 の範囲で秒単位の値を指定します。デフォルト値は 90 です。0 時に設定すると、デバイスは BSS スイッチオーバー要求を送信した直後にクライアントから切断されます。推奨スイッチオーバーが設定されている場合、デバイスは BSS スイッチオーバー要求を送信した後にクライアントとの接続を切断しません。

説明

bss transition-management disassociation コマンドは、BSS スイッチの関連付け解除機能を有効にします。

undo bss transition-management disassociation コマンドは、BSS スイッチの関連付け解除機能をオフにします。

BSS ハンドオーバアソシエーション解除機能を設定した後、デバイスが無線クライアントから BSS ハンドオーバ問い合わせを受信すると、無線クライアントに BSS ハンドオーバを要求するメッセージを発行し、クライアントを BSS ハンドオーバに誘導します。

クライアントに BSS スイッチオーバーを強制するように設定されている場合、設定されている BSS スイッチオーバーの関連付け解除時刻を過ぎてもクライアントが終了しないと、デバイスはクライアントからの接続を強制的に切断します。この機能は注意して使用してください。

BSS スイッチの関連付け解除は、BSS スイッチ管理機能がオンになっている場合にのみ有効になります。

例

#BSS カットオーバーアソシエーション解除機能を有効にし、強制 BSS カットオーバーアソシエーション解除時間を 60 秒に設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] bss transition-management disassociation forced timer 60

関連コマンド

- **bss transition-management**

2.1.3 ft enable

Syntax

ft enable

undo ft enable

デフォルト

FT 機能はオフになっています。

View

Service template view

定義済みユーザロール

network-admin

説明

ft enable コマンドを使用して、FT (Fast BSS Transition、高速 BSS スイッチオーバー)機能を有効にします。

undo ft enable コマンドを使用して、FT 機能をオフにします。

FT の主な目的は、ローミング中のクライアントの遅延時間を短縮することです。FT を使用して、同じ ESS で同じモバイルドメイン内のクライアントの高速ローミングを実現できます。クライアントが 802.11r 高速ローミングを行うとき、クライアントはネゴシエートされた情報を最初に関連付ける必要があります。

FT を有効にする場合、サービステンプレートが無効であることを確認してください。

FT を有効にするサービステンプレートは、security-ie rsn、client association-location ac を使用し、WPA3 と enhanced-open が無効である必要があります。

例

#FT 機能をオンにします。

<Sysname> system-view

[Sysname] wlan service-template st

[Sysname-wlan-st-st] ft enable

関連コマンド

- **security-ie**

2.1.4 ft mobility-domain-id

Syntax

ft mobility-domain-id *mobility-domain-id*

undo ft mobility-domain-id

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

mobility-domain-id:モビリティドメイン ID を 1 から 65535 の範囲で指定します。

説明

ft mobility-domain-id を使用して、デバイスのモビリティドメイン ID を指定します。

undo ft mobility-domain-id を使用して、デフォルトに戻します。

このコマンドを実行すると、クライアントが異なるデバイス間を切り替えるときに、クライアントのアクセス時間を短縮できます。

このコマンドを実行すると、2 つのデバイスが同じモビリティドメイン ID を持つ場合、クライアントは高速 BSS 遷移 (FT) を介して異なるデバイス間をローミングできます。

FT が有効でモビリティグループに含まれていないデバイス間でクライアントが切り替える場合、クライアントはデバイス間 FT ローミングを使用することがあります。ただし、デバイスがモビリティグループに含まれていないため、デバイス間ローミングは失敗します。その後、クライアントはアソシエーションによって新しいデバイスに切り替えます。デバイス間 FT ローミングを試行せずにクライアントが新しいデバイスに直接関連付けられるように、デバイスに異なるモビリティドメイン ID を設定できます。その結果、デバイス間 FT ローミングプロセスが省略されるため、サービススイッチオーバー時間が短縮されます。

このコマンドは、ワイヤレスサービステンプレートを有効にする前に実行します。このコマンドは、FT が有効な場合にのみ有効です。

例

Specify mobility domain ID 666 for the device.

<Sysname> system-view

[Sysname] wlan service-template st

[Sysname-wlan-st-st] ft mobility-domain-id 666

関連コマンド

- **ft enable**

2.1.5 ft reassociation-timeout

Syntax

ft reassociation-timeout *timeout*

undo ft reassociation-timeout

デフォルト

アソシエーションのタイムアウトは 20 秒です。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

timeout:相関タイムアウトを秒単位で 1~100 の範囲で指定します。

説明

ft reassociation-timeout コマンドを使用して、アソシエーションのタイムアウト時間(クライアントが認証を完了した後、クライアントがアソシエーション要求を開始する最大間隔)を設定します。

undo ft reassociation-timeout コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、サービステンプレートが有効になっておらず、FT 機能が有効になっている場合にのみ設定できます。

アソシエーションのタイムアウト時間内にクライアントがアソシエーションを開始しなかった場合、ローミングは終了します。

例

#相関タイムアウトを 30 秒に設定します。

<Sysname> system-view

[Sysname] wlan service-template st

[Sysname-wlan-st-st] ft reassociation-timeout 30

関連コマンド

- **ft enable**

2.1.6 mac-authentication fast-connect enable

Syntax

mac-authentication fast-connect enable

undo mac-authentication fast-connect enable

デフォルト

MAC アドレス認証が成功した後の高速接続機能はオフになっています。

View

Service template view

定義済みユーザロール

network-admin

説明

mac-authentication fast-connect enable コマンドは、MAC アドレス認証が成功した後に高速接続機能を有効にするために使用します。

undo mac-authentication fast-connect enable コマンドは、MAC アドレス認証が成功した後で高速接続機能を無効にするために使用します。

MAC アドレス認証成功後の高速接続機能を起動した後、すでに MAC アドレス認証を通過したクライアントが AC 内でローミングする時、再度 MAC アドレス認証を行う必要がなく、これによってクライアント AC 内ローミングの上り速度を向上させる。

この機能は、AC で認証および関連付けられているワイヤレスクライアントにのみ有効です。

AC 間ローミングで MAC アドレス認証を行うクライアントの場合、このコマンドを設定すると、クライアントはローミング VLAN を継承できますが、ローミングステータスは N/A と表示されます。同じローミンググループ内の AC アップストリームインターフェイスは、クライアントが属する VLAN が AC 間ローミングで異なる場合に、MAC アドレス認証のためにクライアント VLAN を通過させる必要があります。

このコマンドは、ワイヤレスサービステンプレートがオフの場合にのみ設定できます。

例

#ワイヤレスサービステンプレート service1 で、MAC アドレス認証が成功した後の高速接続を有効にします。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] mac-authentication fast-connect enable

関連コマンド

- **client-security authentication-mode (ユーザアクセスと認証)**

2.1.7 sacp anti-sticky

Syntax

sacp anti-sticky { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] [**forced-logoff**] }

undo sacp anti-sticky

デフォルト

Radio view では、無線は AP group's radio view の設定を使用します。

AP group's radio view では、クライアントの anti-sticky が有効になっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

rssi *rssi-value*:RSSI しきい値を 5 から 100 dBm の範囲で指定します。デフォルトのしきい値は 20 dBm です。

interval *interval*:検出間隔を 1 秒から 10 秒の範囲で指定します。デフォルトでは、間隔は 3 秒です。

forced-logoff:信号強度が RSSI しきい値より低い 802.11v 以外のクライアントをログオフします。

説明

sacp anti-sticky enable コマンドを使用して、クライアントの anti-sticky を有効にします。

sacp anti-sticky disable コマンドを使用して、クライアントの anti-sticky を無効にします。

undo sacp anti-sticky コマンドを使用して、デフォルトに戻します。

この機能により、AP は指定された間隔でクライアントの信号強度を調べることができます。802.11v クライアントの場合、クライアントの信号強度がしきい値よりも低い場合、関連付けられた AP は BSS 移行をトリガーしてクライアントをより良い BSS に誘導します。802.11v 以外のクライアントの場合、アクションは実行されません。

例

#クライアントのアンチスティッキを有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、AP ap 1 の無線 1 の強制ログオフを有効にします。

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] sacp anti-sticky enable rssi 30 interval 5 forced-logoff

#クライアントのアンチスティッキを有効にし、RSSI しきい値を 30 に設定し、AP グループ 1 の AP の無線 1 の検出間隔を 5 秒に設定します。

<Sysname> system-view

[Sysname] wlan ap-group 1

[Sysname-wlan-ap-group-1] ap-model QX-W1020

[Sysname-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[Sysname-wlan-ap-group-1-ap-model-QX-W1020-radio-1] sacp anti-sticky enable rssi 30 interval 5

関連コマンド

- **bss transition-management**

目次

このセクションのページは **10-x-x** です。

3 章 モビリティグループ 3-1
3.1 モビリティグループ設定コマンド 3-1
3.1.1 authentication-mode 3-1
3.1.2 display wlan mobility 3-2
3.1.3 display wlan mobility group 3-3
3.1.4 group enable 3-4
3.1.5 member 3-6
3.1.6 snmp-agent trap enable wlan mobility 3-7
3.1.7 source 3-8
3.1.8 tunnel-type 3-9
3.1.9 wlan mobility group 3-9
3.1.10 wlan mobility-group-isolation enable 3-10

3章 モビリティグループ

3.1 モビリティグループ設定コマンド

3.1.1 authentication-mode

Syntax

authentication-mode authentication-mode { **cipher** | **simple** } string

undo authentication-mode

デフォルト

IADTP 制御メッセージの整合性を検証しません。

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

authentication-mode:認証モードを指定します。128 ビットの MD 5 認証モードのみがサポートされます。

cipher:暗号化形式でキーを指定します。

simple:平文形式でキーを指定します。セキュリティのため、平文形式で指定されたキーは暗号化された形式で保存されます。

string:キーを指定します。プレーンテキスト形式は、大文字と小文字を区別する 1 から 16 文字の文字列です。暗号化形式は、大文字と小文字を区別する 33 から 53 文字の文字列です。

説明

authentication-mode コマンドを使用して、IADTP 制御メッセージの認証モードを設定します。

undo authentication-mode コマンドを使用して、デフォルトに戻します。

このコマンドを使用して、デバイスが IADTP トンネルを介して送信される制御メッセージの整合性を確認できるようにします。

例

#認証モードを MD 5 に設定し、プレーンテキストのキーを 12345 に設定します。

<Sysname> system-view

[Sysname] wlan mobility group aaa

[Sysname-wlan-mg-aaa] authentication-mode md5 simple 12345

3.1.2 display wlan mobility

Syntax

display wlan mobility { **roam-in** | **roam-out** } [**member ip** ipv4-address]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

roam-in:別のデバイスから現在のデバイスにローミングしたクライアントを指定します。

roam-out:別のデバイスにローミングしたクライアントを指定します。

member ip *ipv 4-address*:メンバーデバイスの IPv 4 アドレスを指定します。

説明

display wlan mobility コマンドを使用して、デバイスとの間でローミングされたクライアントに関する情報を表示します。

メンバーデバイスが指定されていない場合、このコマンドは別のデバイスとの間でローミングされたすべてのクライアントに関する情報を表示します。

例

#デバイスにローミングしたすべてのクライアントに関する情報を表示します。
<Sysname> display wlan mobility roam-in

```
Total entries: 1
MAC address    BSSID         VLAN ID  HA IP address
5250-0012-0411  cbab-abab-abab  1       192.168.0.101
```

#指定したメンバーデバイスにローミングしたクライアントの情報を表示します。
<Sysname> display wlan mobility roam-in member ip 192.168.0.101

```
Total entries: 1
MAC address    BSSID         VLAN ID
5250-0012-0411  cbab-abab-abab  1
```

#別のデバイスにローミングしたすべてのクライアントに関する情報を表示します。
<Sysname> display wlan mobility roam-out

```
Total entries: 1
MAC address    BSSID         VLAN ID  Online time      FA IP address
```

```
5250-0012-0411  cbab-abab-abab  1       00hr 01min 39sec  192.168.0.102
```

#指定したメンバーデバイスから別のデバイスにローミングしたクライアントの情報を表示します。

[Sysname] display wlan mobility roam-out member ip 192.168.0.102

```
Total entries: 1
MAC address    BSSID          VLAN ID  Online time
5250-0012-0411  cbab-abab-abab  1       00hr 03min 02sec
```

表 3-1 display wlan mobility コマンドの表示情報の説明

フィールド	説明
Total entries	クライアントの総数
MAC address	クライアントのMACアドレス
BSSID	クライアントが関連付けられているAPのBSSID
VLAN ID	クライアントのVLAN ID
HA IP address	HAのIPアドレス
FA IP address	FAのIPアドレス
Online time	クライアントのオンライン時間

3.1.3 display wlan mobility group

Syntax

display wlan mobility group

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan mobility group コマンドを使用して、モビリティグループ情報を表示します。

例

#モビリティグループの情報を表示します。

<Sysname> display wlan mobility group

```
Mobility group name: office
 Tunnel type: IPv4
 Source IPv4: 172.16.220.101
```

```
Source IPv6: Not configured
Authentication method: Not configured
Auto discovery: Enabled
Mobility group status: Enabled
Member entries: 3
IP address                          State        Online duration
172.16.220.102                       DOWN         00hr 00min 00sec
172.16.220.105                       UP           00hr 36min 27sec
172.16.220.106                       UP (A)        00h 50min 30sec
```

表 3-2 display wlan mobility group コマンドの表示情報の説明

フィールド	説明
Tunnel type	モビリティグループのIADTPトンネルタイプ: • IPv4 • IPv6 IPv6 は、現在のソフトウェアバージョンではサポートされていません。
Authentication method	モビリティグループに使用される認証方式。
Auto discovery	グループメンバーの自動検出の状態: • Enabled • Disabled
Mobility group status	モビリティグループのステータス: • Enabled • Disabled
Member entries	メンバーデバイスの数
IP address	メンバーデバイスのIPアドレス
State	IADTPトンネルの状態: • UP • DOWN サフィックス (A) は、デバイスがグループメンバーの自動検出によってグループに参加したことを示します
Online duration	メンバーデバイスのオンライン期間

関連コマンド

- **wlan mobility group**

3.1.4 group enable

Syntax

group enable

undo group enable

デフォルト

無効

View

Mobility group view

定義済みユーザロール

network-admin

説明

モビリティグループを有効にするには、**group enable** コマンドを使用します。

モビリティグループを無効にするには、**undo group enable** コマンドを使用します。

モビリティグループを有効にする前に、次のタスクを完了していることを確認してください。

- IADTP トンネルアドレスタイプと同じタイプの送信元 IP アドレスを設定します。
- IADTP トンネルアドレスタイプと同じタイプのメンバーIP アドレスを指定するか、グループメンバーの自動検出を有効にします。

この機能により、デバイスは IADTP トンネルを確立し、ローミングエントリをメンバーデバイスと同期できます。

デバイスでモビリティグループを無効にすると、デバイスはすべてのメンバーデバイスで確立されたすべての IADTP トンネルをシャットダウンし、ローミングエントリを削除します。

例

#モビリティグループ floor 1 を有効にします。

<Sysname> system-view

[Sysname] wlan mobility group floor1

[Sysname-wlan-mg-floor1] tunnel-type ipv4

[Sysname-wlan-mg-floor1] source ip 192.168.0.1

[Sysname-wlan-mg-floor1] member ip 192.168.0.2

[Sysname-wlan-mg-floor1] group enable

例

- **member**
- **source**
- **tunnel-type**
- **wlan mobility group**

3.1.5 member

Syntax

member ip ipv4-address [**vlan** vlan-id-list]

デフォルト

設定なし

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ip *ipv 4-address*:IPv 4 アドレスでデバイスを指定します。

vlan *vlan-id-list*:最大 10 個の VLAN 項目のスペース区切りリストを指定します。各項目は、*vlan-id 1* から *vlan-id 2* の形式で、VLAN ID または VLAN ID の範囲を指定します。VLAN ID の値の範囲は 2 から 4094 です。*vlan-id 2* 引数の値を *vlan-id 1* 引数の値より小さくすることはできません。

説明

member コマンドを使用して、モビリティグループメンバーを追加します。

undo member コマンドを使用して、モビリティグループメンバーを削除します。

このコマンドを使用する前に、モビリティグループが無効になっていることを確認してください。

モビリティグループ内のメンバーは、IADTP トンネルの確立に使用される IP アドレスによって識別されます。

デバイスは、1 つのモビリティグループにのみ所属できます。

モビリティグループには、最大 31 の IPv 4 メンバーを追加できます。

メンバーデバイスの VLAN を指定すると、モビリティグループ内の他のメンバーデバイスが、指定された VLAN からメンバーデバイスのクライアントデータを直接転送できるようになります。メンバーデバイスの VLAN を指定しない場合、そのクライアントデータは、クライアントがそのメンバーにローミングしない限り、モビリティグループ内の他のメンバーから直接転送できません。

モビリティグループに複数のデバイスがある場合は、モビリティグループ内のメンバー間の IADTP トンネルにループが存在しないことを確認します。

パラメータを指定しない場合、このコマンドの undo 形式は、モビリティグループ内のすべてのメンバーデバイスを削除します。

例

#モビリティグループのメンバーを追加します。

<Sysname> system-view

[Sysname] wlan mobility group abc

[Sysname-wlan-mg-abc] member ip 192.168.1.55 vlan 3 10 19 22 to 30

3.1.6 snmp-agent trap enable wlan mobility

Syntax

snmp-agent trap enable wlan mobility

undo snmp-agent trap enable wlan mobility

デフォルト

WLAN ローミングのアラーム機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

WLAN ローミングのアラーム機能を有効にするには、**snmp-agent trap enable wlan mobility** コマンドを使用します。

WLAN ローミングのアラーム機能をオフにするには、**undo snmp-agent trap enable wlan mobility** コマンドを使用します。

WLAN ローミングモジュールのアラーム機能をオンにすると、モジュールの重要なイベントを報告するアラーム情報が生成されます。生成されたアラーム情報はデバイスの SNMP モジュールに送信され、SNMP 内のアラーム情報の送信パラメータを設定することにより、アラーム情報の出力に関する属性が決定されます。警告の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

例

#WLAN ローミングのアラーム機能を有効にします。

<Sysname> system-view

[Sysname] snmp-agent trap enable wlan mobility

3.1.7 source

Syntax

source ip ipv4-address

undo source［ **ip** ］

デフォルト

設定なし

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*:送信元 IPv 4 アドレスを指定します。

説明

source コマンドを使用して、IADTP トンネルを確立するための送信元 IP アドレスを指定します。

undo source コマンドを使用して、IADTP トンネルを確立するための送信元 IP アドレスを削除します。

デバイスは、送信元 IP アドレスを使用して、メンバーデバイスとの IADTP トンネルを確立します。

モビリティグループが無効になっていることを確認します。

undo コマンドを使用するときに IP アドレスを指定しなかった場合、このコマンドはすべての送信元 IP アドレスを削除します。

例

#IADTP トンネルを確立するための送信元 IPv 4 アドレスを指定します。

<Sysname> system-view

[Sysname] wlan mobility group abc

[Sysname-wlan-mg-abc] source ip 192.168.1.55

関連コマンド

- **group enable**
- **member**

3.1.8 tunnel-type

Syntax

tunnel-type ipv4

undo tunnel-type

デフォルト

IPv4

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ipv4:IPv 4 アドレスタイプを指定します。

説明

IADTP トンネルの IP アドレスタイプを指定するには、**tunnel-type** コマンドを使用します。

デフォルトに戻すには、**undo tunnel-type** コマンドを使用します。

このコマンドを実行する前に、モビリティグループが無効になっていることを確認してください。

例

#モビリティグループ aaa の IADTP トンネルの IP アドレスタイプを IPv 4 で指定します。

<Sysname> system-view

[Sysname] wlan mobility group aaa

[Sysname-wlan-mg-aaa] tunnel-type ipv4

3.1.9 wlan mobility group

Syntax

wlan mobility group group-name

undo wlan mobility group group-name

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name:名前でモビリティグループを指定します。スペースを含まない、大文字と小文字を区別しない 1 から 15 文字の文字列です。

説明

wlan mobility group コマンドを使用して、モビリティグループを作成してそのビューを入力するか、既存のモビリティグループのビューを入力します。

undo wlan mobility group コマンドを使用して、デフォルトに戻します。

メンバーデバイスに設定されているモビリティグループは、同じ名前である必要があります。

1 つのデバイスに作成できるモビリティグループは 1 つだけです。

例

#office という名前のモビリティグループを作成し、そのビューを入力します。

<Sysname> system-view

[Sysname] wlan mobility group office

[Sysname-wlan-mg-office]

3.1.10 wlan mobility-group-isolation enable

Syntax

wlan mobility-group-isolation enable

undo wlan mobility-group-isolation enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan mobility-group-isolation enable コマンドは、モビリティグループのトンネルアイソレーションを有効にします。

undo wlan mobility-group-isolation enable コマンドは、モビリティグループのトンネルアイソレーションを無効にします。

このコマンドは、モビリティグループ内の AP 間にループが存在する場合に必要です。このコマンドにより、AP はモビリティグループ内のトンネル間でパケットを転送できなくなり、ブロードキャストストームが回避されます。

例

#モビリティグループのトンネルアイソレーションを有効にします。

<Sysname> system-view

[Sysname] wlan mobility-group-isolation enable

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

11. WLAN トラフィック最適化

本マニュアルは以下に示す章で構成されています。

01- ユーザアイソレーション

目次

このセクションのページは **11-x-x** です。

1 章 ユーザアイソレーション 1-1
1.1 ユーザアイソレーション設定コマンド 1-1
1.1.1 display user-isolation statistics 1-1
1.1.2 reset user-isolation statistics 1-2
1.1.3 user-isolation enable 1-3
1.1.4 user-isolation permit-broadcast 1-4
1.1.5 user-isolation vlan enable 1-4
1.1.6 user-isolation vlan permit-mac 1-5

1章 ユーザアイソレーション

1.1 ユーザアイソレーション設定コマンド

1.1.1 display user-isolation statistics

Syntax

display user-isolation statistics [**vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*:指定した VLAN のユーザ隔離統計情報を表示します。vlan-id は VLAN 番号で、範囲は 1~4094 です。このパラメータを指定しない場合は、すべての VLAN のユーザ隔離統計情報が表示されます。

説明

display user-isolation statistics コマンドを使用して、VLAN ベースのユーザ分離統計情報を表示します。

例

#すべての VLAN のユーザ隔離統計情報を表示します。

<Sysname> display user-isolation statistics

```
Number of VLANs enabled with user isolation: 2
Number of VLANs disabled with user isolation: 1

VLAN    Status    Drops       Permit-Unicast    Permitted MACs    Permit IPv4|I
Pv6 Acl
4       Enabled   0           Y                 N/A               3001|3002
6       Disabled  0           N                 0023-89a2-3d4d    3001|3002
5       Enabled   0           Y                 N/A               N/A|N/A
```

表1-1 display user-isolation statistics コマンドの表示情報の説明

フィールド	説明
Number of VLANs enabled with user isolation	ユーザ分離機能が有効になっているVLANの数
Number of VLANs disabled with user isolation	ユーザ分離が有効になっていないVLANの数
VLAN	ユーザ隔離を有効にするVLAN ID
State	ユーザ隔離機能の状態: ● Enabled:オン ● Disabled:停止ステータス
Drops	このVLAN内でドロップされたメッセージの数
Permit-Unicast	ユニキャストメッセージの通過がVLAN内で許可されているかどうか。 ● Y:ユニキャストの通過を許可し、ブロードキャスト/マルチキャストのみを分離 ● N:ユニキャスト/ブロードキャスト/マルチキャストの分離
Permitted MAC list	このVLANで許可されているMACアドレスのリスト
Permit IPv4|IPv6 Acl	このVLANで許可されるIPv4 ACLおよびIPv6 ACL

関連コマンド

- **user-isolation vlan enable**
- **user-isolation vlan permit-mac**

1.1.2 reset user-isolation statistics

Syntax

reset user-isolation statistics [**vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*:指定した VLAN 内のユーザ隔離統計情報をクリアします。vlan-id は VLAN 番号で、範囲は 1~4094 です。このパラメータを指定しない場合は、すべての VLAN のユーザ隔離統計情報がクリアされます。

説明

VLAN ベースのユーザ分離統計情報をクリアするには、**reset user-isolation statistics** コマンドを使用します。

例

#VLAN 1 のユーザ分離統計情報をクリアして下さい。

<Sysname> reset user-isolation statistics vlan 1

関連コマンド

- **user-isolation vlan enable**
- **user-isolation vlan permit-mac**

1.1.3 user-isolation enable

Syntax

user-isolation enable

undo user-isolation enable

デフォルト

SSID ベースのユーザ隔離機能はオフになっています。

View

Service template view

定義済みユーザロール

network-admin

説明

user-isolation enable コマンドを使用して、SSID ベースのユーザ隔離機能を有効にします。

undo user-isolation enable コマンドを使用して、SSID ベースのユーザ隔離機能を無効にします。

例

#SSID ベースのユーザ隔離機能を有効にします。

<Sysname> system-view

[Sysname] wlan service-template 1

[Sysname-wlan-st-1] user-isolation enable

1.1.4 user-isolation permit-broadcast

Syntax

user-isolation permit-broadcast

undo user-isolation permit-broadcast

デフォルト

有線ユーザが無線ユーザに送信するブロードキャストメッセージとマルチキャストメッセージを分離します。

View

System view

定義済みユーザロール

network-admin

説明

user-isolation permit-broadcast コマンドは、有線ユーザがワイヤレスユーザに送信するブロードキャストおよびマルチキャストメッセージの受信を許可するために使用されます。

undo user-isolation permit-broadcast コマンドを使用して、デフォルトの状態を復元します。

有線ユーザと無線ユーザが同じ VLAN に属している場合は、有線ユーザが無線ユーザに送信するブロードキャストメッセージとマルチキャストメッセージを分離し、有線ユーザが無線ユーザに送信するブロードキャストメッセージとマルチキャストメッセージを受信できるようにする必要があります。

例

#有線ユーザがワイヤレスユーザに送信するブロードキャストおよびマルチキャストメッセージを受信できるように設定します。

<Sysname> system-view

[Sysname] user-isolation permit-broadcast

関連コマンド

- **user-isolation vlan enable**

1.1.5 user-isolation vlan enable

Syntax

user-isolation vlan *vlan-list* **enable** [**permit-unicast**]

undo user-isolation vlan *vlan-list* **enable**

デフォルト

VLAN ベースのユーザ分離機能はオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-list:ユーザ隔離機能がオンになっている VLAN の範囲を示す VLAN リスト。vlan-list ={vlan-id1 [to vlan-id2]}&<1-10>で表され、vlan-id は 1~4094 の範囲の値を取り、vlan-id2 は vlan-id1 以上の値を取り、&<1-10>は前のパラメータが 10 回まで入力できることを示します。

permit-unicast:ユニキャストを分離せず、ブロードキャストとマルチキャストのみを分離することを示す。このパラメータが指定されていない場合は、ユニキャスト、ブロードキャスト、およびマルチキャストが分離されます。

説明

user-isolation vlan enable コマンドを使用して、指定した VLAN のユーザ分離機能を有効にします。

undo user-isolation vlan enable コマンドを使用して、指定した VLAN のユーザ分離機能をオフにします。

指定した VLAN でユーザ分離が有効になった後にネットワークが切断されることを回避するには、**user-isolation vlan permit-mac** コマンドに従って、ユーザゲートウェイの MAC アドレスをユーザ分離許可リストに追加してから、その VLAN のユーザ分離を有効にする必要があります。

user-isolation vlan enable コマンドを複数回実行した場合、ユーザ分離機能が有効になっている VLAN は、複数回構成で指定された VLAN の集合です。同じ VLAN が複数回設定されている場合は、最後の設定が有効になります。

例

#VLAN 1 でユーザ隔離を有効にする。

<Sysname> system-view

[Sysname] user-isolation vlan 1 enable

1.1.6 user-isolation vlan permit-mac

Syntax

user-isolation vlan *vlan-list* **permit-mac** *mac-list*

undo user-isolation vlan *vlan-list* **permit-mac** { *mac-list* | **all** }

デフォルト

指定された VLAN の MAC アドレス許可転送リストが設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-list:VLAN リスト。vlan-list ={vlan-id1 [to vlan-id2]}&<1-10>で表され、vlan-id は 1~4094 の範囲の値を取り、vlan-id2 は vlan-id1 以上の値を取り、&<1-10>は前のパラメータが 10 回まで入力できることを示します。

mac-list:MAC アドレス H-H-H 形式の MAC アドレス許可転送リスト。1 つの VLAN 内で最大 64 個の許可された MAC アドレスを設定できます。この MAC アドレスは、ブロードキャストアドレスまたはマルチキャストアドレスとしては許可されません。

all:指定した VLAN のすべての許可 MAC アドレスを削除します。

説明

user-isolation vlan permit-mac コマンドを使用して、指定した VLAN の MAC アドレス許可転送リストを設定します。

undo user-isolation permit-mac コマンドを使用して、指定した VLAN の MAC アドレス許可転送リストを削除します。

指定した VLAN の MAC アドレスを設定してリストを転送できるようにします。この VLAN でユーザ分離機能が有効になっている場合、設定した MAC アドレスは分離されません。

user-isolation vlan permit-mac コマンドを複数回実行する場合は、VLAN で許可される MAC アドレスを、複数回設定された MAC アドレスの集合として指定します。

VLAN ごとに最大 64 個の許可 MAC アドレスを設定でき、一度に最大 16 個の許可 MAC アドレスを設定できます。

例

#設定 VLAN 1 許可される MAC アドレスは 00 bb-ccdd-eeff および 0022-3344-5566 です。

<Sysname> system-view

[Sysname] user-isolation vlan 1 permit-mac 00bb-ccdd-eeff 0022-3344-5566

関連コマンド

- **display user-isolation statistics**
- **user-isolation vlan enable**

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

12. WLAN アドバンスド機能

本マニュアルは以下に示す章で構成されています。

01- WLAN 最適化

02- WLAN メッシュ

03- IoT 機能

04- HotSpot2.0 の設定

目次

このセクションのページは **12-x-x** です。

1 章 WLAN 最適化 1-1
1.1 WLAN 最適化設定コマンド 1-1
1.1.1 option broadcast-multicast-buffer 1-1
1.1.2 option client reconnect 1-2
1.1.3 option client hide-node-protection 1-4
1.1.4 option keep-active 1-4
1.1.5 rrop anti-bmc network 1-6
1.1.6 rrop anti-bmc rate-limit 1-7
1.1.7 rrop anti-bmc rate-limit pps 1-8
1.1.8 rrop anti-bmc upstream client-rate-limit 1-9
1.1.9 rrop anti-bmc upstream client-rate-limit pps 1-11
1.1.10 rrop client fast-keep-alive 1-12
1.1.11 rrop flow-schedule mode 1-13
1.1.12 rrop software-retry 1-15

1章 WLAN 最適化

1.1 WLAN最適化設定コマンド

1.1.1 option broadcast-multicast-buffer

Syntax

option broadcast-multicast-buffer { disable | enable [limit limit] }

undo option broadcast-multicast-buffer

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view で、マルチキャスト/ブロードキャストメッセージキャッシュ機能がオンになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

limit *limit*:キャッシュされたマルチキャスト/ブロードキャストメッセージの数を 1~600 の範囲で設定します。デフォルト値は 100 です。

説明

option broadcast-multicast-buffer enable コマンドを使用して、マルチキャスト/ブロードキャストメッセージキャッシュ機能を有効にします。

option broadcast-multicast-buffer disable コマンドを使用して、マルチキャスト/ブロードキャストメッセージキャッシュ機能をオフにします。

undo option broadcast-multicast-buffer コマンドを使用して、デフォルトの状態を復元します。

マルチキャスト/ブロードキャストメッセージキャッシュ機能が有効になっている場合、AP は、WLAN ネットワーク内の関連する無線クライアントがスリープ状態にあることを検出すると、送信するマルチキャストまたはブロードキャストメッセージをキャッシュし、一定時間後にブロードキャストおよびマルチキャストメッセージを送信します。

リアルタイムのマルチキャストトラヒックに対して、マルチキャストメッセージをキャッシュすることは、ネットワーク全体のマルチキャストメッセージがキャッシュされてから送信される過程を経て、他の非休眠状態の無線クライアントに影響を与える。

マルチキャスト/ブロードキャストメッセージキャッシュ機能をオフにすると、AP が送信するすべてのマルチキャスト、ブロードキャストメッセージはスリープ中の無線クライアントの影響を受けなくなり、マルチキャストとブロードキャストメッセージの迅速かつタイムリーな送信を実現する。

例

#マルチキャスト/ブロードキャストメッセージキャッシュ機能をオフにします。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option broadcast-multicast-buffer disable

#マルチキャスト/ブロードキャストメッセージキャッシュ機能をオフにします。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] option broadcast-multicast-buffer disable

1.1.2 option client reconnect

Syntax

option client reconnect { disable | enable [rssi rssi-value] [interval interval] }

undo option client reconnect

デフォルト

Radio view では、AP グループの設定を引き継ぎます。

AP group's radio view では、アクティブなトリガークライアント再接続機能はオフになっています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

rssi *rssi-value*:無線クライアントの信号強度のしきい値は 5~100 の範囲で、デフォルト値は 10、推奨値は 20 です。

interval *interval*:無線クライアントの信号強度をプローブする間隔。範囲は 3~10 で、単位は秒、デフォルト値は 3 です。

説明

option client reconnect enable コマンドを使用して、クライアント再接続をアクティブにトリガーします。

option client reconnect disable コマンドは、クライアント再接続のアクティブなトリガーをオフにします。

undo option client reconnect コマンドを使用して、デフォルトの状態を復元します。

本機能を起動した後、無線クライアントの信号強度が持続的に弱くなり、かつ閾値を下回る時、AP は自発的に無線クライアントに認証解除フレームメッセージを送信し、無線クライアントに再接続またはローミングの機会を与える。

例

#アクティブ起動クライアント再接続機能を起動し、アクセス信号強度閾値を 30 に設定し、クライアント信号強度を探査する時間間隔を 5 秒に設定する。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option client reconnect enable rssi 30 interval 5

#アクティブ起動クライアント再接続機能を起動し、アクセス信号強度閾値を 30 に設定し、クライアント信号強度を探査する時間間隔を 5 秒に設定する。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] option client reconnect enable rssi 30 interval 5

1.1.3 option client hide-node-protection

Syntax

option client hide-node-protection { **disable** | **enable** }

undo option client hide-node-protection

デフォルト

Radio view では、AP グループの設定を引き継ぎます。

AP group's radio view では、隠れ端末保護は無効です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

disable：隠れ端末保護を無効にします。

enable：隠れ端末保護を有効にします。

説明

option client hide-node-protection enable コマンドは、隠れ端末保護を有効にします。

option client hide-node-protection disable コマンドは、隠れ端末保護を無効にします。

undo option client hide-node-protection コマンドはデフォルトの状態に戻します。

このコマンドは、802.11g、802.11n、802.11ac、802.11ax クライアントにのみ適用可能です。

この機能を有効にすると、クライアントは隠れ端末からの干渉を避けるために RTS/CTS フレームを送信します。

本機能によって複数端末の通信衝突を軽減させることが可能です。

Radio view での設定は、AP group radio view での設定より優先されます。

1.1.4 option keep-active

Syntax

option keep-active { **disable** | **enable** }

undo option keep-active

デフォルト

Radio view では、AP グループの設定を引き継ぎます。

AP group's radio view では、無線クラアントのスリープ時間を短縮する機能は無効です。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

説明

option keep-active enable コマンドは、無線クライアントのスリープ時間を短縮する機能を有効にします。

option keep-active disable コマンドは、無線クライアントのスリープ時間を短縮する機能を無効にします。

undo option keep-active コマンドはデフォルトの状態に戻します。

スリープ状態の無線クライアントは、ビーコンフレーム内の TIM（トラフィック通知メッセージ）情報を定期的にリスニングすることで、接続している AP が無線クライアントのパケットをバッファしているかどうかを判断します。AP が無線クライアントのパケットをバッファしている場合、スリープ状態は終了し、AP とデータ通信を行います。本機能を有効にすると、AP はビーコンフレーム内の TIM を変更し、端末のスリープ時間を短縮して、伝送効率を向上させます。

例

ap1 で無線クライアントのスリープ時間短縮機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] option keep-active enable

#apgroup1 でクライアントのスリープ時間短縮機能を有効にします。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-group-apgroup1] ap-model QX-W1110

[AC-wlan-ap group-apgroup1-ap-model-QX-W1110] radio 1

[AC-wlan-ap group-apgroup1-ap-model-QX-W1110] option keep-active enable

1.1.5 rrop anti-bmc network

Syntax

rrop anti-bmc network { disable | { ipv4-simple | ipv6-simple | ipv4-and-ipv6-simple } enable }

undo rrop anti-bmc network

デフォルト

AP view:AP グループ設定を継承します。

AP group view:IPv4 ネットワーク基本ブロードキャストとマルチキャストメッセージ制御がオンになっています。

パラメータ

ipv4-simple:IPv4 ネットワーク基本メッセージ。

ipv6-simple:IPv6 ネットワーク基本メッセージ。

ipv4-and-ipv6-simple:IPv4 および IPv6 ネットワークの基本メッセージ。

View

AP view

AP group view

定義済みユーザロール

network-admin

説明

rrop anti-bmc network enable コマンドは、ネットワークでブロードキャストとマルチキャストのメッセージ制御を有効にします。

rrop anti-bmc network disable コマンドは、ネットワークのブロードキャストとマルチキャストのメッセージ制御機能を無効にします。

undo rrop anti-bmc network コマンドを使用して、デフォルトの状態を復元します。

IPv4 ネットワーク基本放送とマルチキャストメッセージ制御機能をオンにした後、AP がダウンストリームで放送とマルチキャストメッセージを受信した後、APはローカルで ARP 放送メッセージに応答し、DHCP 放送要求メッセージを廃棄し、他の IPv4 基本放送とマルチキャストメッセージを正常に処理する。

IPv6 ネットワーク基本放送とマルチキャストメッセージ制御機能を起動した後、AP が下りで放送とマルチキャストメッセージを受信した後、AP はローカルで RS メッセージと DHCPv6 放送要求メッセージを廃棄し、RA メッセージをユニキャストに転送し、NS メッセージに応答して応答し、その他の IPv6 基本放送とマルチキャストメッセージを正常に処理する。

この機能は、ソフトウェア転送のみをサポートし、ハードウェア転送はサポートしません。

例

#IPv4 ネットワーク基本ブロードキャストとマルチキャストメッセージ制御を有効にします。(AP view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] rrop anti-bmc network ipv4-simple enable

#IPv4 ネットワーク基本ブロードキャストとマルチキャストメッセージ制御を有効にします。(AP group view)

<AC> system-view

[AC] wlan ap-group group1

[AC-ap-group-group1] rrop anti-bmc network ipv4-simple enable

1.1.6 rrop anti-bmc rate-limit

Syntax

rrop anti-bmc { broadcast | } **multicast** rate-limit { disable | enable }

undo rrop anti-bmc { broadcast | multicast } rate-limit

デフォルト

AP view:AP グループ設定を継承します。

AP group view:メッセージ制限機能がオフになっています。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

broadcast:ブロードキャストメッセージ。

multicast:マルチキャストメッセージ。

説明

rrop anti-bmc rate-limit enable コマンドは、メッセージ速度制限を有効にします。

rrop anti-bmc rate-limit disable コマンドは、メッセージ速度制限をオフにします。

undo rrop anti-bmc rate-limit コマンドを使用して、デフォルトの状態を復元します。

この機能は、AP がブロードキャストおよびマルチキャストメッセージをダウンストリームで送信するレートを制限し、Radio インターフェイスの有効使用率を向上させるために使用されます。

例

#ブロードキャストメッセージの速度制限を有効にします。(AP view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] rrop anti-bmc broadcast rate-limit enable

#ブロードキャストメッセージの速度制限機能を有効にします。(AP group view)

<AC> system-view

[AC] wlan ap-group group1

[AC-ap-group-group1] rrop anti-bmc broadcast rate-limit enable

関連コマンド

- **rrop anti-bmc rate-limit pps**

1.1.7 rrop anti-bmc rate-limit pps

Syntax

rrop anti-bmc { broadcast | multicast } rate-limit pps max-pps

undo rrop anti-bmc { broadcast | multicast } rate-limit *pps*

デフォルト

AP view:AP グループ設定を継承します。

AP group view:メッセージのダウンストリームスロットルレートが設定されていません。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

broadcast:ブロードキャストメッセージ。

multicast:マルチキャストメッセージ。

pps *max-pps*:AP が 1 秒あたりに送信できるドロップパケットの最大数。範囲は 1~141 万です。

説明

rrop anti-bmc rate-limit pps コマンドを使用して、メッセージのダウンストリームレートを設定します。

undo rrop anti-bmc rate-limit pps コマンドを使用して、デフォルトの状態を復元します。

メッセージレート制限機能がオンの場合、このコマンドを設定すると、AP が上下に送信するメッセージレートが制限値を超えると、AP はレート制限を超えるメッセージをドロップします。

例

#ブロードキャストメッセージのダウンストリームレートを毎秒 1024 メッセージに設定します。(AP view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] rrop anti-bmc broadcast rate-limit pps 1024

#ブロードキャストメッセージのダウンストリームレートを毎秒 1024 メッセージに設定します。(AP group view)

<AC> system-view

[AC] wlan ap-group group1

[AC-ap-group-group1] rrop anti-bmc broadcast rate-limit pps 1024

関連コマンド

- **rrop anti-bmc rate-limit**

1.1.8 rrop anti-bmc upstream client-rate-limit

🕮 **メモ：**

- **rrop anti-bmc upstream client-rate-limit** コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。
- **disable** パラメータは System view では指定できません。

Syntax

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit enable

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit disable

undo rrop anti-bmc { broadcast | multicast } upstream client-rate-limit

デフォルト

AP view：AP group view の設定を使用します。AP group view に設定がない場合、AP は System view の設定を使用します。

AP group view：System view の設定を使用します。

System view：無効

View

AP view

AP group view

System view

定義済みユーザロール

network-admin

パラメータ

broadcast: アップリンクのブロードキャストパケットのレートを制限します。

multicast: アップリンクのマルチキャストパケットのレートを制限します。

説明

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit enable コマンドはアップリンクのブロードキャストまたはマルチキャストパケットのレート制限を有効にします。

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit disable コマンドはアップリンクのブロードキャストまたはマルチキャストパケットのレート制限を無効にします。

undo rrop anti-bmc { broadcast | multicast } upstream client-rate-limit コマンドはデフォルトに戻します。

このコマンドは、制限するレートの値を指定した場合にのみ有効です。

例

System view でアップリンクのブロードキャストパケットのレートを制限します。

<AC> system-view

[AC] rrop anti-bmc broadcast upstream client-rate-limit enable

#AP group 1 でアップリンクのブロードキャストパケットのレートを制限します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rrop anti-bmc broadcast upstream client-rate-limit enable

1.1.9 rrop anti-bmc upstream client-rate-limit pps

🕮 **メモ：**

- **rrop anti-bmc upstream client-rate-limit pps** コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

rrop anti-bmc { broadcast | multicast } upstream client-rate-limit pps *max-pps*

undo rrop anti-bmc { broadcast | multicast } upstream client-rate-limit pps

デフォルト

AP view：AP group view の設定を使用します。AP group view に設定がない場合、AP は System view の設定を使用します。

AP group view：System view の設定を使用します。

System view：AP が各クライアントからブロードキャストもしくはマルチキャストパケットを受信するレートに制限はありません。

View

AP view

AP group view

System view

定義済みユーザロール

network-admin

パラメータ

broadcast: ブロードキャストパケットのレートを制限します。

multicast: マルチキャストパケットのレートを制限します。

pps *max-pps*: AP が各クライアントから 1 秒あたりに受信できるブロードキャストまたはマルチキャストパケットの最大数を 1～1410000 の範囲で指定します。AP は、指定された制限を超えるブロードキャストまたはマルチキャストパケットを破棄します。

説明

rrop anti-bmc upstream client-rate-limit pps コマンドは AP が各クライアントからブロードキャストまたはマルチキャストパケットを受信するレートの最大数を設定します。

undo rrop anti-bmc upstream client-rate-limit pps コマンドはデフォルトに戻します。

例

AP が各クライアントから 1 秒あたりに受信できるブロードキャストパケットの最大数を System view で 1024 に制限します

<AC> system-view

[AC] rrop anti-bmc broadcast upstream client-rate-limit pps 1024

1.1.10 rrop client fast-keep-alive

Syntax

rrop client fast-keep-alive { disable | enable [count count-value] [interval interval-value] }

undo rrop client fast-keep-alive

デフォルト

Radio view:AP グループ設定を継承します。

AP group's radio view:有効

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

count **count-value**: キープアライブカウントを 128~2048 の範囲で指定します。デフォルト値は 450 です。

interval **interval-value**: キープアライブ間隔を 3~60 秒の範囲で指定します。デフォルト値は 10 です。

説明

rrop client fast-keep-alive enable コマンドはクライアント高速キープアライブを有効にします。

rrop client fast-keep-alive disable コマンドはクライアント高速キープアライブを無効にします。

undo rrop client fast-keep-alive コマンドはデフォルトに戻します。

クライアントの高速キープアライブ機能は、クライアントにユニキャストパケットを送信するように AP を設定することで、クライアントのオンラインステータスを迅速に確認します。AP は、ユニキャストパケットをキープアライブパケットとして扱い、カウント値のユニキャストパケットを 1 つのグループに含めます。AP はユーザーデータを 3 つのグループに分けて個別にカウントします。キープアライブ期間 (interval-value) 内に、AP がクライアントから 3 つのグループのユニキャストパケットに対して応答を受信しない場合、AP はクライアントがオンラインでないと判断します。AP はクライアントをログオフして、無線リソースの使用率を向上させます。

このコマンドは、主にクライアントのモビリティが高いシナリオで使用されます。ネットワークの品質が低い場合は、AP がクライアントに送信できるキープアライブパケットの最大数を減らすか、キープアライブ間隔を短くします。ベストプラクティスとして、クライアントが安定しているシナリオではデフォルト設定を使用します。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#AP グループ 1 の QX-W1120 の Radio1 のクライアントの高速キープアライブを有効にし、キープアライブ数を 300 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1120

[AC-wlan-ap-group-1-ap-model-QX-W1120] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1120-radio-1] rrop client fast-keep-alive enable count 300

1.1.11 rrop flow-schedule mode

🕮 **メモ：**

- **rrop flow-schedule mode** コマンドはソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。
- この機能と、クライアントのレート制限機能が同時に設定されている場合、**client-rate-limit** コマンドを使用して設定された無線クライアントレート制限が有効になります。

Syntax

rrop flow-schedule mode { **balanced** | **quick-speed** | **intelligent** [**channel-usage-threshold** *threshold-value* | **max** *max-value* | **min** *min-value*] }

undo rrop flow-schedule mode

デフォルト

AP view：AP group view の設定を使用します。

AP group view：**quick-speed** モード

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

Balanced：バランスモードを指定します。このモードでは、AC はクライアントに帯域幅を均等に割り当てます。

quick-speed：**quick-speed** モードを指定します。このモードでは、クライアントが自分のトラフィックに基づいて帯域幅を競います。

Intelligent：インテリジェントモードを指定します。このモードでは、AC はクライアントに帯域幅を均等に割り当て、アイドリングクライアントの余剰帯域幅を大きなトラフィックのクライアントにアルゴリズム計算に基づいて再割り当てできます。

channel-usage-threshold *threshold-value* **:**インテリジェントスケジューリングのしきい値を 1 から 99 の範囲で指定します。チャネル使用率が設定されたしきい値以上になると、インテリジェントスケジューリングモードが自動的に有効になります。

チャネル使用率がしきい値を下回ると、インテリジェントスケジューリングモードが自動的に無効になります。インテリジェントスケジューリングしきい値を指定しない場合、インテリジェントスケジューリングモードは常に有効になります。

max *max-value* **:** 最大クライアント速度を 16 から 1700000Kbps の範囲で指定します。

min *min-value* **:** 最小クライアント速度を 16 から 1700000Kbps の範囲で指定します。最大クライアント速度は最小クライアント速度より高い値を設定します。

説明

rrop flow-schedule mode コマンドは AP のトラフィックスケジューリングモードを設定します。

undo rrop flow-schedule mode コマンドはデフォルトに戻します。

例

#AP ap1 の radio 1 のトラフィックスケジューリングモードをインテリジェントモードに設定します。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rrop flow-schedule mode Intelligent

#AP グループ 1 の QX-W1240 の Radio1 のトラフィックスケジューリングモードを quick-speed モードに設定します。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1240

[AC-wlan-ap-group-1-ap-model-QX-W1240] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1240-radio-1] rrop flow-schedule mode quick-speed

1.1.12 rrop software-retry

Syntax

rrop software-retry { unicast [eap] | broadcast-multicast } enable count count

rrop software-retry { unicast [eap] | broadcast-multicast } disable

undo rrop software-retry { unicast [eap] | broadcast-multicast }

デフォルト

Radio view の下で、AP グループ設定を引き継ぎます。

AP group's radio view の下で、すべてのタイプのメッセージの再送信数はデバイスモデルに関連しています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

unicast:ユニキャストメッセージの再送信回数を設定します。

eap:eap メッセージの再送回数を設定します。

broadcast-multicast:マルチキャストの再送信回数を設定します。

count *count*:メッセージの再送回数を 1~16 の範囲で設定する。

説明

rrop software-retry enable コマンドは、ソフトウェアのメッセージ再送信機能を有効にします。

rrop software-retry disable コマンドは、ソフトウェアのメッセージ再送信機能を無効にします。

undo rrop software-retry コマンドを使用して、デフォルトの状態を復元します。

例

#復元 eap メッセージの再送回数はデフォルトの構成です。(Radio view)

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] undo rrop software-retry unicast eap

#回復ブロードキャストメッセージの再送回数はデフォルトの構成である。(AP group's radio view)

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1020

[AC-wlan-ap-group-1-ap-model-QX-W1020] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1020-radio-1] undo rrop software-retry broadcast-multicast

目次

このセクションのページは **12-x-x** です。

2 章 WLAN メッシュの設定 2-1
2.1 WLAN メッシュコマンド 2-1
2.1.1 akm mode sae 2-1
2.1.2 display wlan mesh-link ap 2-2
2.1.3 display wlan mesh-policy 2-4
2.1.4 display wlan mesh-profile 2-5
2.1.5 interface wlan-mesh 2-6
2.1.6 link-hold-rssi 2-7
2.1.7 link-initiation enable 2-8
2.1.8 link-keepalive 2-9
2.1.9 link-maximum-number 2-10
2.1.10 link-saturation-rssi 2-11
2.1.11 mesh peer-mac-address 2-12
2.1.12 mesh-id 2-13
2.1.13 mesh-interface 2-14
2.1.14 mesh-peer intra-ac-mpp enable 2-15
2.1.15 mesh-policy 2-16
2.1.16 mesh-port access vlan 2-18
2.1.17 mesh-port hybrid pvid 2-19
2.1.18 mesh-port hybrid vlan 2-20
2.1.19 mesh-port link-type 2-22
2.1.20 mesh-port trunk permit vlan 2-23
2.1.21 mesh-port trunk pvid 2-24
2.1.22 mesh-profile 2-25
2.1.23 mesh-profile enable 2-27
2.1.24 portal-service enable 2-27
2.1.25 preshared-key 2-29
2.1.26 probe-request-interval 2-30
2.1.27 temporary-link enable 2-31
2.1.28 wlan mesh-policy 2-31
2.1.29 wlan mesh-profile 2-32

2章 WLAN メッシュの設定

2.1 WLAN メッシュコマンド

2.1.1 akm mode sae

Syntax

akm mode sae

undo akm mode

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

説明

akm mode sae コマンドは akm（authentication and key management）モードを SAE（simultaneous authentication of equals）に設定します。

undo akm mode コマンドはデフォルトに戻します。

akm モードを設定する、あるいは削除する前に、メッシュプロファイルが無効であることを確認してください。

例

メッシュプロファイル 1 の akm モードを SAE に設定します。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] akm mode sae

関連コマンド

display wlan mesh-profile

2.1.2 display wlan mesh-link ap

Syntax

display wlan mesh-link ap [**name** *ap-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。大文字と小文字を区別します。

verbose: メッシュリンクの詳細情報を表示します。このパラメータを指定しない場合、簡易情報を表示します。

説明

display wlan mesh-link コマンドはメッシュリンク情報を表示します。

パラメータを指定しない場合、すべてのメッシュリンクの情報を表示します。

例

AP **ap1** のメッシュリンクの簡易情報を表示します。

<AC> display wlan mesh-link ap name ap1

```
AP name: ap1
 Peer          Local         Status     RSSI  Packets(Rx/Tx)
 4ab7-c78a-22ff  75bb-c36d-4ef8  Forwarding  22    0/0
```

表 2-1 コマンド出力

フィールド	説明
Peer	ピアMPのMACアドレス
Local	ローカルAPのMACアドレス
Status	リンクのステータス。メッシュリンクがトラフィックを転送している場合、**Forwarding**と表示されます。
RSSI	メッシュリンクのRSSI
Packets(Rx/Tx)	メッシュリンクのパケット統計情報： ● **Rx**－受信パケット数

フィールド	説明
	• Tx－送信パケット数

すべての AP のメッシュリンクの詳細情報を表示します。

<AC> display wlan mesh-link ap verbose

```
AP name: ap1
 Peer MAC               : 84d9-317d-9710
 Local MAC              : 70f9-6dd7-cf00
 Status                 : Forwarding
 Link mode              : dot11an
 RSSI                   : 67
 SNR                    : 67
 Noise                  : 0 dBm
 Cost                   : 0
 Incorrect packet         : 0.00 %
 Packets
   Received             : 1508
   Sent                 : 14617
   Resent               : 162
   Lost                 : 0

AP name: ap2
 Peer MAC               : 84d9-317d-9710
 Local MAC              : 0606-e203-1111
 Status                 : Forwarding
 Link mode              : dot11an
 RSSI                   : 62
 SNR                    : 62
 Noise                  : 0 dBm
 Cost                   : 0
 Incorrect packet         : 0.03 %
 Packets
   Received             : 2921
   Sent                 : 2877
   Resent               : 178
   Lost                 : 1
```

表 2-2 コマンド出力

フィールド	説明
Peer MAC	ピアMPのMACアドレス
Local MAC	ローカルAPのMACアドレス

フィールド	説明
Status	リンクのステータス。メッシュリンクがトラフィックを転送している場合、**Forwarding**と表示されます。
Link mode	無線モード
RSSI	メッシュリンクのRSSI
SNR	信号対雑音比
Cost	リンクコスト
Incorrect packets	送信エラーが発生した送信パケットの割合
Received	受信パケットの総数
Sent	送信されたパケットの総数
Resent	再送信されたパケット数
Lost	ロスしたパケット数

2.1.3 display wlan mesh-policy

Syntax

display wlan mesh-policy [*mesh-policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mesh-policy-name: 大文字と小文字を区別しない 1～31 文字でメッシュポリシ名を指定します。ポリシ名を指定しない場合、すべてのメッシュポリシの情報を表示します。

説明

display wlan mesh-policy コマンドはメッシュポリシ情報を表示します。

例

全てのメッシュポリシの情報を表示します。

<AC> display wlan mesh-policy

```
Mesh policy name                 : default_mesh_policy
Mesh link initiation              : Enabled
Max links                        : 2
Probe request interval            : 1000 ms
```

```
Link hold RSSI                  : 15
```

表 2-3 コマンド出力

フィールド	説明
Mesh link initiation	メッシュリンク開始機能の状況： ● 有効 ● 無効
Max links	リンクの最大数
Link hold RSSI	メッシュリンクホールドRSSI

2.1.4 display wlan mesh-profile

Syntax

display wlan mesh-profile [*mesh-profile-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mesh-profile-number: メッシュプロファイルの番号を指定します。値の範囲は 1～32 です。メッシュプロファイルを指定しない場合、すべてのメッシュプロファイルの情報を表示します。

説明

display wlan mesh-profile コマンドはメッシュプロファイル情報を表示します。

例

全てのメッシュプロファイルの情報を表示します。

<AC> display wlan mesh-profile

```
Mesh profile number         : 1
Mesh ID                    : 11
Link keepalive interval     : 2 s
Link backhaul rate         : 18 Mbps
Mesh profile status         : Enabled
Link metric type           : Not Configured
AKM mode                   : None
```

```
PSK status                : Disabled

Mesh profile number         : 2
Mesh ID                   : 22
Link keepalive interval     : 2 s
Link backhaul rate          : 18 Mbps
Mesh profile status         : Enabled
Link metric type           : Not Configured
AKM mode                  : None
PSK status                : Disabled
```

表 2-4 コマンド出力

フィールド	説明
Mesh profile status	メッシュプロファイルの状況： ● 有効 ● 無効
AKM mode	akmモード ● None－akmモードは指定されていません。 ● SAE－SAEモードが指定されています。
PSK status	事前共有鍵設定状況： ● Enabled－事前共有鍵が設定されています。 ● Disabled－事前共有鍵は設定されていません。

2.1.5 interface wlan-mesh

Syntax

interface wlan-mesh *interface-number*

undo interface wlan-mesh *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: メッシュインタフェースの番号を指定します。値の範囲は 0～1023 です。

説明

interface wlan-mesh コマンドはメッシュインタフェースを作成し、その view に移行します。あるいは既存のメッシュインタフェースの view に移行します。

undo interface wlan-mesh コマンドはメッシュインタフェースを削除します。

例

AP **ap1** にメッシュインタフェース 1 を作成し、WLAN メッシュインタフェース view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1030

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-mesh1]

AP グループ **g1** のすべての AP にメッシュインタフェース 2 を作成し、AP グループ view の WLAN メッシュインタフェース view に移行します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2]

関連コマンド

mesh-interface

2.1.6 link-hold-rssi

Syntax

link-hold-rssi *value*

undo link-hold-rssi

デフォルト

15 dBm

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

value: メッシュリンクホールド RSSI を指定します。値の範囲は 5～100dBm です。

説明

link-hold-rssi コマンドはメッシュリンクホールド RSSI（メッシュリンクを保持するための最小信号強度）を設定します。

undo link-hold-rssi コマンドはデフォルトに戻します。

例

メッシュリンク **abc** に対してメッシュリンクホールド RSSI を 24dBm に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-hold-rssi 24

関連コマンド

display wlan mesh-policy

2.1.7 link-initiation enable

Syntax

link-initiation enable

undo link-initiation enable

デフォルト

有効

View

Mesh policy view

定義済みユーザロール

network-admin

説明

link-initiation enable コマンドはメッシュリンク開始を有効にします。

undo link-initiation enable コマンドはメッシュリンク開始を無効にします。

メッシュリンク開始を有効にすることで、MP はリンクオープン要求を送信していないピアに対してリンクオープン要求を送信します。この機能が無効の場合、MP はピアがリンクオープン要求を送信するまで、ピアに対してリンクオープン要求を送信しません。

例

メッシュリンク開始を無効にします。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] undo link-initiation enable

関連コマンド

display wlan mesh-policy

2.1.8 link-keepalive

Syntax

link-keepalive *keepalive-interval*

undo link-keepalive

デフォルト

2 秒

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

keepalive-interval: keepalive 間隔を指定します。値の範囲は 1～1800 秒です。

説明

link-keepalive コマンドはメッシュリンク keepalive 間隔を設定します。

undo link-keepalive コマンドはデフォルトに戻します。

メッシュリンクの MP はメッシュリンク状態を検出するために keepalive パケットを使用します。大きい MAC アドレスをもつ MP は、keepalive 間隔で keepalive パケットをピアの端に送信します。keepalive パケットを送信した MP は、連続して 3 回の keepalive 間隔終了前に応答を受信しない場合、メッシュリンクを切断します。また、keepalive パケットを受信した MP は、連続して 3 回の keepalive 間隔終了前に keepalive パケットを

受信しない場合、メッシュリンクを切断します。リンク状態を正しく検出するため、送信側の keepalive 間隔は、受信側の keepalive 間隔の 3 倍以下に設定してください。

例

メッシュプロファイル 1 でメッシュリンク keepalive 間隔を 6 秒に設定します。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] link-keepalive 6

関連コマンド

display wlan mesh-profile

2.1.9 link-maximum-number

🕮 **メモ：**

ホップ数（ネットワーク内のメッシュリンクの最長経路）が増加するにつれてスループットは低下します。

Syntax

link-maximum-number *max-link-number*

undo link-maximum-number

デフォルト

2

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

max-link-number: メッシュリンクの最大数を指定します。値の範囲は 1～8 です。

説明

link-maximum-number コマンドは無線のメッシュリンクの最大数を設定します。

undo link-maximum-number コマンドはデフォルトに戻します。

MP はメッシュリンクが最大数に達すると、無線での新規メッシュリンクの確立を停止します。

例

メッシュポリシ **abc** に対してメッシュリンクの最大数を 5 に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-maximum-number 5

関連コマンド

display wlan mesh-policy

2.1.10 link-saturation-rssi

Syntax

link-saturation-rssi *value*

undo link-saturation-rssi

デフォルト

150 dBm

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

value: リンク飽和 RSSI 値を 30～150 dBm の範囲で指定します。

説明

link-saturation-rssi コマンドはリンク飽和 RSSI を設定します。

undo link-saturation-rssi コマンドはデフォルトに戻します。

強力な信号強度がチップのパフォーマンスに影響を与えないように、リンクの RSSI がリンク飽和 RSSI を超えた場合に MP はアクティブ リンクを終了します。

例

メッシュポリシ **abc** に対して、リンク飽和 RSSI を 50 dBm に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] link-saturation-rssi 50

関連コマンド

display wlan mesh-policy

2.1.11 mesh peer-mac-address

Syntax

Radio view:

mesh peer-mac-address [**blacklist**] { *mac-address* | **disable** }

undo mesh peer-mac-address [**blacklist**] [*mac-address*]

AP group's radio view:

mesh peer-mac-address [**blacklist**] *mac-address*

undo mesh peer-mac-address [**blacklist**] [*mac-address*]

デフォルト

Radio view：AP group's radio view の設定を使用します。

AP group's radio view：設定なし

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

blacklist: MP の MAC アドレスをメッシュピアブラックリストに追加します。このパラメータを指定しない場合､MAC アドレスはメッシュピアホワイトリストに追加されます。

mac-address: MP の MAC アドレスを H-H-H 形式で指定します。

説明

mesh peer-mac-address コマンドはメッシュピアブラックリストもしくはホワイトリストに MP を追加します。

mesh peer-mac-address disable コマンドはすべての MP からメッシュピアブラックリストもしくはホワイトリストを削除し、AP が AP グループ view の設定を引き継がないようにします。

undo mesh peer-mac-address コマンドはメッシュピアブラックリストもしくはホワイトリストから MP を削除します。

ブラックリストとホワイトリストの両方を設定した場合、ホワイトリストのみ適用されます。

同じ MAC アドレスをホワイトリストもしくはブラックリストに追加するために、このコマンドを複数回実行した場合、最後の設定が適用されます。

Radio view の設定は AP group's radio view の設定より優先されます。

例

AP **ap1** のメッシュピアホワイトリストに MP の MAC アドレスを追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh peer-mac-address 4ab7-c78a-22ff

AP **ap1** のメッシュピアブラックリストに MP の MAC アドレスを追加します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh peer-mac-address blacklist 4ab7-c78a-22ff

AP グループ **g1** の AP のメッシュピアホワイトリストに MP の MAC アドレスを追加します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1030

[AC-wlan-ap-group-g1-ap-model-QX-W1030] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-W1030-radio-1] mesh peer-mac-address 4ab7-c78a-22ff

2.1.12 mesh-id

Syntax

mesh-id *mesh-id*

undo mesh-id

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

mesh-id: メッシュ ID を指定します。大文字と小文字を区別する 1～32 文字で指定できます。

説明

mesh-id コマンドはメッシュプロファイルにメッシュ ID に割り当てます。

undo interface wlan-mesh コマンドはデフォルトに戻します。

例

メッシュプロファイル 1 にメッシュ ID を割り当てます。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] mesh-id mesh

関連コマンド

display wlan mesh-profile

2.1.13 mesh-interface

Syntax

Radio view:

mesh-interface { *interface-number* | **disable** }

undo mesh-interface

AP group's radio view:

mesh-interface *interface-number*

undo mesh-interface

デフォルト

Radio view：AP group's radio view の設定を使用します。

AP group's radio view：設定なし

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

interface-number: メッシュインタフェースの番号を指定します。値の範囲は 0～1023 です。

説明

mesh-interface コマンドは無線にメッシュインタフェースをバインドします。

mesh-interface disable コマンドは無線からメッシュインタフェースのバインドを解除し、AP が AP group's radio view の設定を引き継がないようにします。

undo mesh-interface コマンドはデフォルトに戻します。

無線にバインドできるメッシュインタフェースは 1 つだけです。このコマンドを複数回実行すると、最新のバインドが有効になります。

AP view で作成されたメッシュインタフェースは、Radio view でのみ無線にバインドできます。AP group's radio view で作成されたメッシュインタフェースは、Radio view と AP group's radio view の両方で無線にバインドできます。

例

AP **ap1** の radio 1 にメッシュインタフェース 1 をバインドします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-interface 1

AP グループ **g1** の AP の radio 1 にメッシュインタフェース 2 をバインドする。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1030

[AC-wlan-ap-group-g1-ap-model-QX-W1030] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-W1030-radio-1] mesh-interface 2

関連コマンド

interface wlan-mesh

2.1.14 mesh-peer intra-ac-mpp enable

Syntax

mesh-peer intra-ac-mpp enable

undo mesh-peer intra-ac-mpp enable

デフォルト

ループを防ぐため、同一の AC に関連付いている MPP はメッシュピアになることはできません。

View

Global configuration view

定義済みユーザロール

network-admin

説明

mesh-peer intra-ac-mpp enable コマンドは同一の AC に関連付いた MPP がメッシュピアになることを有効にします。

undo mesh-policy コマンドはデフォルトに戻します。

同一の AC に関連付いた MPP が VLAN1 でメッシュリンクを確立しないようにしてください。

例

同一の AC に関連付いた MPP がメッシュピアになるように設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] mesh-peer intra-ac-mpp enable

2.1.15 mesh-policy

Syntax

Radio view:

mesh-policy name { **default** | **name** *policy-name* }

undo mesh-policy

AP group’s radio view:

mesh-policy name *policy-name*

undo mesh-policy

デフォルト

Radio view：AP group’s radio view の設定を使用します。

AP group’s radio view：デフォルトメッシュポリシの **default_mesh_policy** が無線にバインドされています。

View

Radio view

AP group's radio view

定義済みユーザロール

network-admin

パラメータ

policy-name: メッシュポリシ名を指定します。大文字と小文字を区別しない 1～31 文字で指定できます。

default: デフォルトメッシュポリシの **default_mesh_policy** を指定します。

説明

mesh-policy コマンドはメッシュポリシを無線にバインドします。

undo mesh-policy コマンドはデフォルトに戻します。

1 つの無線に 1 つのメッシュポリシをバインドできます。このコマンドを複数回実行した場合、最後に実行したものが適用されます。

Radio view の設定は AP group's radio view の設定より優先されます。

例

AP **ap1** の radio 1 にメッシュポリシ **policy1** をバインドします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-policy name policy1

AP グループ **g1** の AP の radio1 にメッシュポリシ **policy2** をバインドします。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-W1030

[AC-wlan-ap-group-g1-ap-model-QX-W1030] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-W1030-radio-1] mesh-policy name policy2

AP **ap1** の radio 1 にデフォルトメッシュポリシをバインドします。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-policy default

関連コマンド

wlan mesh-policy

2.1.16 mesh-port access vlan

Syntax

mesh-port access vlan *vlan-id*

undo mesh-port access vlan

デフォルト

VLAN 1

View

WLAN-mesh interface view

AP group's WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を 1～4094 の範囲で指定します。

説明

mesh-port access vlan コマンドはアクセスタイプのメッシュインタフェースに VLAN を割り当てます。

undo mesh-port access vlan コマンドはデフォルトに戻します。

このコマンドを実行する前に、VLAN が存在することを確認してください。

例

AP **ap1** の WLAN メッシュ 1 に VLAN 2 を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port access vlan 2

AP グループ **g1** の AP の WLAN メッシュ 2 に VLAN 2 を割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port access vlan 2

関連コマンド

- **interface wlan-mesh**
- **remote-configuration enable**

2.1.17 mesh-port hybrid pvid

Syntax

mesh-port hybrid pvid vlan *vlan-id*

undo mesh-port hybrid pvid

デフォルト

ハイブリッドポートの PVID は、ポートのリンクタイプがアクセスだったときに属していた VLAN の値です。

View

WLAN-mesh interface view

AP group's WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を 1～4094 の範囲で指定します。

説明

mesh-port hybrid pvid vlan コマンドはハイブリッドタイプのメッシュインタフェースの PVID を設定します。

undo mesh-port hybrid pvid コマンドはハイブリッドタイプのメッシュインタフェースの PVID を VLAN 1 に設定します

2 つの MP が互いにメッシュリンクを確立するために使用するメッシュインタフェースが同じ PVID を持っていることを確認してください。

ハイブリッドポートがポート VLAN からパケットを転送できるように、ハイブリッドポートにポート VLAN を割り当ててください。

例

AP **ap1** の WLAN メッシュ 1 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type hybrid

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port hybrid pvid vlan 100

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port hybrid vlan 100 untagged

#AP グループ **g1** の AP の WLAN メッシュ 2 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type hybrid

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port hybrid pvid vlan 100

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port hybrid vlan 100 untagged

関連コマンド

- **mesh-port hybrid vlan**
- **mesh-port link-type**

2.1.18 mesh-port hybrid vlan

Syntax

mesh-port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo mesh-port hybrid vlan *vlan-id-list*

デフォルト

ハイブリッドポートは、ポートのリンクタイプがアクセスのときに属していた VLAN のタグなしメンバです。

View

WLAN-mesh interface view

AP group's WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: スペースで区切られた VLAN の値を最大 10 個まで指定します。各項目は VLAN ID、もしくは VLAN ID の範囲を vlan-id1 から vlan-id2 の形式で指定します。VLAN

ID の値の範囲は 1～4094 です。vlan-id2 パラメータの値は、vlan-id1 パラメータの値以上である必要があります。指定した VLAN は、装置に既に存在している必要があります。

tagged: 指定した VLAN のタグ付きメンバとしてポートを設定します。VLAN のタグ付きメンバは、VLAN タグを削除せずに VLAN からパケットを送信します。

untagged: 指定した VLAN のタグなしメンバとしてポートを設定します。VLAN タグを削除した後、VLAN のタグなしメンバが VLAN からパケットを送信します。

説明

mesh-port hybrid vlan コマンドはハイブリッドタイプのメッシュインタフェースに VLAN を割り当てます。

undo mesh-port hybrid vlan コマンドは指定された VLAN からハイブリッドタイプのメッシュインタフェースを除外します。

ハイブリッドポートでは、複数の VLAN を許可できます。ハイブリッドポートでこのコマンドを複数回実行すると、ハイブリッドポートは指定された VLAN をすべて許可します。

例

AP **ap1** で WLAN メッシュ 1 をハイブリッドポートとして作成し、タグ付きメンバとして VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type hybrid

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port hybrid vlan 2 4 50 to 100 tagged

AP グループ **g1** の AP で WLAN メッシュ 2 をハイブリッドポートとして作成し、タグ付きメンバとして VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type hybrid

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

- **mesh-port hybrid pvid**
- **mesh-port link-type**

2.1.19 mesh-port link-type

Syntax

mesh-port link-type { **access** | **hybrid** | **trunk** }

undo mesh-port link-type

デフォルト

アクセスポート

View

WLAN-mesh interface view

AP group's WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートリンクタイプをアクセスに設定します。

hybrid: ポートリンクタイプをハイブリッドに設定します。

trunk: ポートリンクタイプをトランクに設定します。

説明

mesh-port link-type コマンドはメッシュインタフェースのリンクタイプを設定します。

undo mesh-port link-type コマンドはデフォルトに戻します。

ポートのリンクタイプをトランクとハイブリッド間で変更する場合、まずアクセスポートに設定する必要があります。

例

AP **ap1** で WLAN メッシュ 1 をトランクポートに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type trunk

AP グループ **g1** の AP で WLAN メッシュ 2 をトランクポートに設定します。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type trunk

2.1.20 mesh-port trunk permit vlan

Syntax

mesh-port trunk permit vlan { *vlan-id-list* | **all** }

undo mesh-port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

VLAN 1

View

WLAN-mesh interface view

AP group's WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: スペースで区切られた VLAN の値を最大 10 個まで指定します。各項目は VLAN ID、もしくは VLAN ID の範囲を vlan-id1 から vlan-id2 の形式で指定します。VLAN ID の値の範囲は 1～4094 です。vlan-id2 パラメータの値は、vlan-id1 パラメータの値以上である必要があります。指定した VLAN は、装置に既に存在している必要があります。

tagged: 指定した VLAN のタグ付きメンバとしてポートを設定します。VLAN のタグ付きメンバは、VLAN タグを削除せずに VLAN からパケットを送信します。

untagged: 指定した VLAN のタグなしメンバとしてポートを設定します。VLAN タグを削除した後、VLAN のタグなしメンバが VLAN からパケットを送信します。

説明

mesh-port trunk permit vlan コマンドはトランクタイプのメッシュインタフェースに VLAN を割り当てます。

undo mesh-port trunk permit vlan コマンドは指定された VLAN からトランクタイプのメッシュインタフェースを除外します。

トランクポートでは、複数の VLAN を許可できます。トランクポートでこのコマンドを複数回実行すると、トランクポートは指定された VLAN をすべて許可します。

トランクポートでは、PVID からのパケットのみがタグなしで通過できます。

例

AP **ap1** で WLAN メッシュ 1 をトランクポートとして作成し、VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port link-type trunk

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port trunk permit vlan 2 4 50 to 100

AP グループ **g1** の AP で WLAN メッシュ 2 をトランクポートとして作成し、VLAN 2、VLAN 4、VLAN 50～VLAN 100 を割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port link-type trunk

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port trunk permit vlan 2 4 50 to 100

関連コマンド

- **mesh-port link-type**
- **mesh-port trunk pvid**

2.1.21 mesh-port trunk pvid

Syntax

mesh-port trunk pvid *vlan-id*

undo mesh-port trunk pvid

デフォルト

トランクポートの PVID は VLAN 1 です。

View

WLAN-mesh interface view

AP group's WLAN-mesh interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を 1～4094 の範囲で指定します。

説明

mesh-port trunk pvid コマンドはトランクタイプのメッシュインタフェースの PVID を設定します。

undo mesh-port trunk pvid コマンドはデフォルトに戻します。

存在しない VLAN をトランクポートのポート VLAN として指定できます。

2 つの MP が互いにメッシュリンクを確立するために、使用するメッシュインタフェースが同じ PVID を持っていることを確認してください。

トランクポートがポート VLAN からパケットを送信できるようにするには、トランクポートをポート VLAN に割り当てる必要があります。

例

#AP **ap1** の WLAN メッシュ 1 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] interface wlan-mesh 1

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port trunk pvid vlan 100

[AC-wlan-ap-ap1-wlan-mesh-1] mesh-port trunk permit vlan 100

#AP グループ **g1** の AP の WLAN メッシュ 2 の PVID を VLAN 100 に設定し、タグなしメンバとして割り当てます。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] interface wlan-mesh 2

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port trunk pvid vlan 100

[AC-wlan-ap-group-g1-wlan-mesh-2] mesh-port trunk permit vlan 100

関連コマンド

- **mesh-port link-type**
- **mesh-port trunk permit vlan**

2.1.22 mesh-profile

Syntax

Radio view:

mesh-profile { *mesh-profile-number* | **disable** }

undo mesh-profile

AP group's radio view:

mesh-profile *mesh-profile-number*

undo mesh-profile

デフォルト

Radio view：AP group's radio view の設定を使用します。

AP group’s radio view：設定なし

View

Radio view

AP group’s radio view

定義済みユーザロール

network-admin

パラメータ

mesh-profile-number: メッシュインタフェースの番号を指定します。値の範囲は 1～32 です。

説明

mesh-profile コマンドはメッシュイプロファイルを作成し、無線にバインドします。

mesh-profile disable コマンドは無線からメッシュプロファイルのバインドを解除し、AP が AP グループの設定を引き継がないようにします。

undo interface wlan-mesh コマンドはデフォルトに戻します。

Radio view の設定は AP group’s radio view の設定より優先されます。

例

AP **ap1** の radio 1 にメッシュプロファイル 1 をバインドします。

<AC> system-view

[AC] wlan ap ap1 model QX-1020

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] mesh-profile 1

AP グループ **g1** の AP の radio 1 にメッシュプロファイル 2 をバインドします。

<AC> system-view

[AC] wlan ap-group g1

[AC-wlan-ap-group-g1] ap-model QX-1020

[AC-wlan-ap-group-g1-ap-model-QX-1020] radio 1

[AC-wlan-ap-group-g1-ap-model-QX-1020-radio-1] mesh-profile 2

関連コマンド

- **mesh-profile enable**
- **wlan mesh-profile**

2.1.23 mesh-profile enable

Syntax

mesh-profile enable

undo mesh-profile enable

デフォルト

無効

View

Mesh profile view

定義済みユーザロール

network-admin

説明

mesh-profile enable コマンドはメッシュプロファイルを有効にします。

undo mesh-profile enable コマンドはメッシュプロファイルを無効にします。

メッシュプロファイルを有効にする前に、メッシュ ID を割り当てる必要があります。

例

メッシュプロファイル 1 を有効にします。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1] mesh-profile enable

関連コマンド

mesh-id

2.1.24 portal-service enable

Syntax

AP view もしくは AP group view:

portal-service { **disable** | **enable** }

undo portal-service

Global configuration view:

portal-service enable

undo portal-service

デフォルト

AP view では、AP group view の設定を使用します。AP group view に設定が存在しない場合、global configuration view の設定を使用します。

AP group view では、global configuration view の設定を使用します。

Global configuration view では、MPP はプローブ要求を送信します。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: MPP がプローブ要求を送信し、AP group view もしくは global configuration view の設定を引き継がないようにします。

enable: MPP がプローブ要求を送信するのを無効にします。

説明

portal-service enable コマンドは MPP がプローブ要求を送信するのを無効にします。

portal-service disable コマンドは MPP がプローブ要求を送信し、AP group view もしくは global configuration view の設定を引き継がないようにします。

undo probe-service コマンドはデフォルトに戻します。

WLAN メッシュネットワークを有線ネットワークに接続するメッシュポイントとして、MPP は多数のメッシュリンクを確立する必要があります。パフォーマンスを維持するために、MPP がネイバ検出のプローブ要求を送信しないように無効にできます。MPP は、他の MP からのプローブ要求にのみ応答します。

例

AP **ap1** でプローブ要求を送信しないようにします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1020

[AC-wlan-ap-ap1] portal-service enable

AP グループ **group1** の AP でプローブ要求を送信しないようにします。

<AC> system-view

[AC] wlan ap-group group1

[AC-wlan-ap-group-group1] portal-service enable

グローバルでプローブ要求を送信しないようにします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] portal-service enable

2.1.25 preshared-key

Syntax

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

pass-phrase: 文字列形式で鍵を設定します。

raw-key: 16 進数形式で鍵を設定します。

cipher: 暗号化形式で鍵を指定します。

simple: 平文形式で鍵を指定します。安全のため、平文形式で指定された鍵は暗号化形式で格納されます。

string: 大文字と小文字を区別する鍵列を指定します。鍵の長さの範囲は以下の通りです。

- **pass-phrase plaintext**－8～63 文字
- **pass-phrase ciphertext**－41～117 文字
- **raw-key plaintext**－64 桁の 16 進数
- **raw-key ciphertext**－117 文字

説明

preshared-key コマンドはメッシュプロファイルに事前共有鍵を追加します。

undo preshared-key コマンドはデフォルトに戻します。

このコマンドを使用する前に、メッシュプロファイルが無効であることを確認してください。

メッシュプロファイルに設定できる事前共有鍵は 1 つです。このコマンドを複数回実行した場合、最後の設定が適用されます。

例

メッシュプロファイル 1 に平文の事前共有鍵 **abcdefghij** を追加します。

<AP> system-view

[AP] wlan mesh-profile 1

[AP-wlan-mesh-profile-1] preshared-key pass-phrase simple abcdefghij

関連コマンド

display wlan mesh-profile

2.1.26 probe-request-interval

Syntax

probe-request-interval *interval-value*

undo probe-request-interval

デフォルト

1000 ミリ秒

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

interval-value: 100～8191 ミリ秒の範囲で間隔を指定します。

説明

probe-request-interval コマンドはプローブ要求間隔を設定します。

undo probe-request-interval コマンドはデフォルトに戻します。

例

メッシュポリシ a**bc** に対してプローブ要求間隔を 500 ミリ秒に設定します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] probe-request-interval 500

関連コマンド

display wlan mesh-policy

2.1.27 temporary-link enable

Syntax

temporary-link enable

undo temporary-link enable

デフォルト

有効

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

interval-value: 100～8191 ミリ秒の範囲で間隔を指定します。

説明

temporary-link enable コマンドはテンポラリメッシュリンクの確立を有効にします。

undo temporary-link enable コマンドはデフォルトに戻します。

例

テンポラリメッシュリンクの確立を有効にします。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc] temporary-link enable

2.1.28 wlan mesh-policy

Syntax

wlan mesh-policy *policy-name*

undo wlan mesh-policy *policy-name*

デフォルト

システム定義のポリシ「**default_mesh_policy**」が存在します。

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: メッシュポリシ名を指定します。大文字と小文字を区別しない 1～31 文字で指定できます。

説明

wlan mesh-policy コマンドはメッシュポリシを作成し、その view に移行します。あるいは既存のメッシュポリシの view に移行します。

undo wlan mesh-policy コマンドはメッシュポリシを削除します。

無線で使用中のメッシュポリシ内の属性設定を削除、修正する前に、無線にバインドされたメッシュプロファイルを無効にしてください。

システム定義のメッシュポリシを修正もしくは削除することはできません。

例

メッシュポリシ **abc** を作成し、その view に移行します。

<AC> system-view

[AC] wlan mesh-policy abc

[AC-wlan-mesh-policy-abc]

2.1.29 wlan mesh-profile

Syntax

wlan mesh-profile *mesh-profile-number*

undo wlan mesh-profile *mesh-profile-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mesh-profile-number: メッシュプロファイルの番号を指定します。値の範囲は 1～32 です。

説明

wlan mesh-profile コマンドはメッシュプロファイルを作成し、その view に移行します。あるいは既存のメッシュプロファイルの view に移行します。

undo wlan mesh-profile コマンドはメッシュプロファイルを削除します。

メッシュプロファイル内の属性設定を修正するには、メッシュプロファイルを無効にする必要があります。

例

メッシュプロファイル 1 を作成し、その view に移行します。

<AC> system-view

[AC] wlan mesh-profile 1

[AC-wlan-mesh-profile-1]

関連コマンド

mesh-profile enable

目次

このセクションのページは **12-x-x** です。

3 章 IoT 機能の設定 3-1
3.1 AeroScout ロケーションの設定コマンド 3-1
3.1.1 display wlan rfid-tracking radio 3-1
3.1.2 rfid-tracking aeroscout 3-2
3.1.3 rfid-tracking aeroscout aggregate-report interval 3-3
3.1.4 rfid-tracking aeroscout engine-address 3-5
3.1.5 rfid-tracking aeroscout engine-detection 3-6
3.1.6 rfid-tracking aeroscout report-mode 3-7
3.1.7 rfid-tracking aeroscout tag-multicast-address 3-9
3.1.8 rfid-tracking aeroscout timestamp 3-10
3.1.9 rfid-tracking aeroscout vendor-port 3-12
3.1.10 rfid-tracking mode 3-13
3.1.11 rfid-tracking radio 3-14
3.2 BLE 機能の設定コマンド 3-15
3.2.1 description 3-15
3.2.2 display wlan module-information 3-16
3.2.3 display iot ble neighbor-information 3-18
3.2.4 iot auto-module 3-19
3.2.5 iot auto-module persistent 3-20
3.2.6 iot auto-module persistent all 3-22
3.2.7 module 3-22
3.2.8 module enable 3-23
3.2.9 module firmware-upgrade 3-24
3.2.10 rfid-tracking ble advertisement 3-26
3.2.11 rfid-tracking ble advertisement { disable | enable } 3-28
3.2.12 rfid-tracking ble advertisement interval 3-29
3.2.13 rfid-tracking ble advertisement mode 3-31
3.2.14 rfid-tracking ble aging-time 3-33
3.2.15 tx-power 3-34
3.2.16 type ble 3-35
3.2.17 wlan execute module reset 3-36
3.3 サーバへの IoT データのレポート設定コマンド 3-37
3.3.1 azure-dps group-symmetric-key 3-37
3.3.2 azure-dps id-scope 3-38
3.3.3 display iot transport-profile 3-39
3.3.4 display iot transport-profile in-use 3-40

3.3.5 iot transport-profile 3-42
3.3.6 iot-transport-profile 3-43
3.3.7 keepalive interval..... 3-44
3.3.8 report interval 3-45
3.3.9 server-url 3-46
3.3.10 transport-profile enable 3-47

3章 IoT 機能の設定

3.1 AeroScoutロケーションの設定コマンド

3.1.1 display wlan rfid-tracking radio

Syntax

display wlan rfid-tracking radio [ap *ap-name* **]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

説明

display wlan rfid-tracking radio コマンドは、ワイヤレスロケーションの無線情報を表示します。

例

#ワイヤレスロケーションの無線情報を表示します。

<AC> display wlan rfid-tracking radio

```
                    Wireless Locating
--------------------------------------------------------------------------
 AP name                      Radio ID   Type
--------------------------------------------------------------------------
 ap1                          1          MU/Tag
 ap2                          1          MU
 ap3                          2          Tag
 ap4                          1          N/A
--------------------------------------------------------------------------
```

表 3-1 コマンド出力

フィールド	説明
Type	検索するデバイスのタイプ : • MU/Tag : MUデバイスとTagデバイスの両方 • MU : MUデバイス • Tag : Tagデバイス • N/A : 検索するデバイスのタイプが指定されていません

3.1.2 rfid-tracking aeroscout

Syntax

rfid-tracking aeroscout { disable | enable }

undo rfid-tracking aeroscout

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 無効

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

rfid-tracking aeroscout enable コマンドは AeroScout ロケーションを有効にします。

rfid-tracking aeroscout disable コマンドは AeroScout ロケーションを無効にします。

undo rfid-tracking aeroscout コマンドはデフォルトに戻します。

この機能により、AP はサポートされているすべてのチャネルをスキャンします。すべてのチャネルにデバイスを配置しない場合は、チャネルスキャンホワイトリストまたはブラックリストを設定します。チャネルスキャンホワイトリストおよびブラックリストの詳細は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*9 無線管理*”の”*7 章 チャネルスキャン*”を参照してください。

AP がロケーションパケットをロケーションサーバに送信するには、AeroScout ロケーションと無線ベースロケーションの両方を有効にする必要があります。

例

AP ap1 で、AeroScout ロケーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout enable

AP グループ 1 の AP で、AeroScout ロケーションを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout enable

#グローバルで、AeroScout ロケーションを有効にします。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout enable

3.1.3 rfid-tracking aeroscout aggregate-report interval

Syntax

rfid-tracking aeroscout aggregate-report interval *interval*

undo rfid-tracking aeroscout aggregate-report interval

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: MU ロケーションパケットを集約せずに送信します

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

interval:集約した MU ロケーションパケットのレポート間隔を 100~600000 ミリ秒の範囲で指定します。

説明

rfid-tracking aeroscout aggregate-report interval コマンドは、MU ロケーションパケットの集約を有効にし、集約した MU ロケーションパケットをレポートする間隔を設定します。

undo rfid-tracking aeroscout aggregate-report interval コマンドはデフォルトに戻します。

デフォルトでは、AP は MU ロケーションパケットを受信するとすぐに、そのパケットをロケーションサーバに報告します。これは多くのネットワークリソースを消費します。

この機能を使用すると、AP は受信した MU ロケーションパケットを 1 つのロケーションパケットに集約し、集約したパケットを指定した間隔でロケーションサーバに報告します。集約パケットのサイズが 1400 バイトに達すると、AP はロケーションパケットを直ちにロケーションサーバに報告します。

この機能は、AeroScout ロケーションモードがスタティックモードの場合にだけ有効です。

例

AP ap1 で、MU ロケーションパケットの集約を有効にし、レポート間隔を 100 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout aggregate-report interval 100

AP グループ 1 の AP で、MU ロケーションパケットの集約を有効にし、レポート間隔を 100 ミリ秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout aggregate-report interval 100

#グローバルで、MU ロケーションパケットの集約を有効にし、レポート間隔を 100 ミリ秒に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout aggregate-report interval 100

関連コマンド

rfid-tracking aeroscout

3.1.4 rfid-tracking aeroscout engine-address

Syntax

rfid-tracking aeroscout engine-address *engine-address* **engine-port** *engine-port*

undo rfid-tracking aeroscout engine-address

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: 設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

engine-address : AeroScout ロケーションサーバの IPv4 アドレスを指定します。

engine-port : AeroScout ロケーションサーバのポート番号を 1~65535 の範囲で指定します。

説明

rfid-tracking aeroscout engine-address コマンドは、AeroScout ロケーションサーバの IPv4 アドレスとポート番号を設定します。

undo rfid-tracking aeroscout engine-address コマンドはデフォルトに戻します。

AP がロケーションサーバと通信するために、ロケーションサーバの IPv4 アドレスとポート番号を指定します。スタティック AeroScout ロケーションが使用されている場合、この機能を設定する必要があります。ダイナミック AeroScout ロケーションが使用されている場合、この機能は有効になりません。

例

AP ap1 で、ロケーションサーバの IPv4 アドレスを 192.168.10.10、ポート番号を 3000 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout engine-address 192.168.10.10 engine-port 3000

AP グループ 1 の AP で、ロケーションサーバの IPv4 アドレスを 192.168.10.10、ポート番号を 3000 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout engine-address 192.168.10.10 engine-port 3000

#グローバルで、ロケーションサーバの IPv4 アドレスを 192.168.10.10、ポート番号を 3000 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout engine-address 192.168.10.10 engine-port 3000

関連コマンド

rfid-tracking aeroscout engine-detection

3.1.5 rfid-tracking aeroscout engine-detection

Syntax

rfid-tracking aeroscout engine-detection { dynamic | static }

undo rfid-tracking aeroscout engine-detection

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view: ダイナミックロケーション

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

dynamic：ダイナミックロケーションを指定します。

static：スタティックロケーションを指定します。

説明

rfid-tracking aeroscout engine-detection コマンドは、AeroScout ロケーションモードを指定します。

undo rfid-tracking aeroscout engine-detection コマンドはデフォルトに戻します。

AeroScout ロケーションには、次のロケーションモードがあります。

- ダイナミックロケーション：AP はロケーションサーバとネゴシエーションを行い、タグのマルチキャスト MAC アドレス、パケット間引きの設定、およびロケーションサーバの IP アドレスとポート番号を取得します。ロケーションサーバは、AP の AeroScout バージョン、MAC アドレス、無線モード、およびチャネル情報を取得します。次に、ロケーションサーバは AP にロケーションパケットを送信するように通知します。
- スタティックロケーション：AP は AC から定義済みのロケーション属性を取得し、ロケーションサーバへのロケーションパケットの送信を開始します。ロケーションサーバが AP によるダイナミックネゴシエーションをサポートしていない場合は、スタティック AeroScout ロケーションを使用します。

例

AP ap1 で、AeroScout ロケーションモードをダイナミックロケーションに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout engine-detection dynamic

AP グループ 1 の AP で、AeroScout ロケーションモードをダイナミックロケーションに設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout engine-detection dynamic

#グローバルで、AeroScout ロケーションモードをダイナミックロケーションに設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout engine-detection dynamic

3.1.6 rfid-tracking aeroscout report-mode

Syntax

rfid-tracking aeroscout report-mode { central | local }

undo rfid-tracking aeroscout report-mode

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view：AP(ローカルレポートモード)

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

central : AC(集中レポートモード)を指定します。

local : AP(ローカルレポートモード)を指定します。

説明

rfid-tracking aeroscout report-mode コマンドは、AeroScout ロケーションパケットのレポートモードを指定します。

undo rfid-tracking aeroscout report-mode コマンドはデフォルトに戻します。

ロケーションサーバにロケーションパケットをレポートするモードには、AC (集中レポートモード) と AP (ローカルレポートモード) があります。AC(集中レポートモード)では、AP は最初にロケーションパケットを AC に送信する必要があります。

例

AP ap1 で、AeroScout ロケーションパケットのレポートモードを AC(集中レポートモード)に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout report-mode central

AP グループ 1 の AP で、AeroScout ロケーションパケットのレポートモードを AC(集中レポートモード)に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout report-mode central

#グローバルで、AeroScout ロケーションパケットのレポートモードを AC(集中レポートモード)に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout report-mode central

3.1.7 rfid-tracking aeroscout tag-multicast-address

Syntax

rfid-tracking aeroscout tag-multicast-address *mac-address*

undo rfid-tracking aeroscout tag-multicast-address

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view：設定なし

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

multicast-address：タグのマルチキャスト MAC アドレスを H-H-H の形式で指定します。

説明

rfid-tracking aeroscout tag-multicast-address コマンドは、タグのマルチキャスト MAC アドレスを指定します。

undo rfid-tracking aeroscout tag-multicast-address コマンドはデフォルトに戻します。

AP は、受信したワイヤレスパケットの宛先 MAC アドレスによってタグを識別します。タグのマルチキャスト MAC アドレスを指定しない場合、AP は受信した 802.11 パケットがすべて MU からのものであると判断します。

スタティック AeroScout ロケーションが設定されている場合、タグのマルチキャスト MAC アドレスの指定が必要です。ダイナミック AeroScout ロケーションが使用されている場合、この機能は有効になりません。

例

AP ap1 で、タグのマルチキャスト MAC アドレスとして 0134-1122-3344 を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout tag-multicast-address 0134-1122-3344

#AP グループ 1 の AP で、タグのマルチキャスト MAC アドレスとして 0134-1122-3344 を設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout tag-multicast-address 0134-1122-3344

#グローバルで、タグのマルチキャスト MAC アドレスとして 0134-1122-3344 を設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout tag-multicast-address 0134-1122-3344

関連コマンド

rfid-tracking aeroscout engine-detection

3.1.8 rfid-tracking aeroscout timestamp

Syntax

rfid-tracking aeroscout timestamp { absolute | relative }

undo rfid-tracking aeroscout timestamp

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view：相対タイムスタンプ

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

absolute：絶対タイムスタンプを指定します。絶対タイムスタンプは、1970 年からの経過時間をミリ秒単位で表します。

relative：相対タイムスタンプを指定します。相対タイムスタンプは、AP が起動してからの経過時間をミリ秒単位で表します。

説明

rfid-tracking aeroscout timestamp コマンドは、MU パケットをカプセル化するタイムスタンプの形式を指定します。

undo rfid-tracking aeroscout timestamp コマンドはデフォルトに戻します。

タグパケットは、相対時間だけでカプセル化できます。MU パケットが相対タイムスタンプと絶対タイムスタンプのどちらでカプセル化されるかは、ロケーションサーバの設定によって異なります。一部のベンダのロケーションサーバは、絶対タイムスタンプでカプセル化された MU パケットだけをサポートしています。

例

AP ap1 で、タイムスタンプの形式を絶対タイムスタンプに設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout timestamp absolute

AP グループ 1 の AP で、タイムスタンプの形式を絶対タイムスタンプに設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout timestamp absolute

#グローバルで、タイムスタンプの形式を絶対タイムスタンプに設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout timestamp absolute

関連コマンド

rfid-tracking aeroscout

3.1.9 rfid-tracking aeroscout vendor-port

Syntax

rfid-tracking aeroscout vendor-port *vendor-port-number*

undo rfid-tracking aeroscout vendor-port

デフォルト

AP view: AP group view の設定を使用します。

AP group view: global configuration view の設定を使用します。

Global configuration view：1144 ポート

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

パラメータ

vendor-port-number :ポート番号を 1~65535 の範囲で指定します。

説明

rfid-tracking aeroscout vendor-port コマンドは、AP がロケーションサーバからのメッセージを受信するポートを指定します。

undo rfid-tracking aeroscout vendor-port コマンドはデフォルトに戻します。

AP がロケーションサーバからのメッセージを受信するポートを指定するには、このコマンドを実行します。スタティック AeroScout ロケーションが設定されている場合、AP は指定されたポートから受信したパケットに応答しません。

例

AP ap1 で、AP がロケーションサーバからのメッセージを受信するポートを 3000 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking aeroscout vendor-port 3000

AP グループ 1 の AP で、AP がロケーションサーバからのメッセージを受信するポートを 3000 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] rfid-tracking aeroscout vendor-port 3000

#グローバルで、AP がロケーションサーバからのメッセージを受信するポートを 3000 に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC- wlan-global-configuration] rfid-tracking aeroscout vendor-port 3000

関連コマンド

- **rfid-tracking aeroscout**
- **rfid-tracking aeroscout engine-detection**

3.1.10 rfid-tracking mode

Syntax

rfid-tracking mode { **mu** | **tag** }

undo rfid-tracking mode { **mu** | **tag** }

デフォルト

Radio view: AP group radio view の設定を使用します。

AP group radio view: 設定なし

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

パラメータ

mu：MU を指定します。

tag：タグを指定します。

説明

rfid-tracking mode コマンドは、検索するデバイスのタイプを指定します。

undo rfid-tracking mode コマンドは、指定されたデバイスのタイプを削除します。

rfid-tracking mode コマンドを実行すると、AP は指定されたタイプのデバイスに関するロケーション情報だけをロケーションサーバに送信します。

このコマンドを複数回実行して、MU とタグの両方を検索するように AP を設定することができます。

例

AP ap1 で、検索するデバイスのタイプを MU に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rfid-tracking mode mu

AP グループ 1 の型番 QX-W1110 の AP で、検索するデバイスのタイプを MU に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-radio-1] rfid-tracking mode mu

関連コマンド

rfid-tracking aeroscout

3.1.11 rfid-tracking radio

Syntax

rfid-tracking radio { **disable** | **enable** }

undo rfid-tracking radio

デフォルト

Radio view: AP group radio view の設定を使用します。

AP group radio view: 無効

View

Radio view

AP group radio view

定義済みユーザロール

network-admin

説明

rfid-tracking radio enable コマンドは、無線ベースのロケーションを有効にします。

rfid-tracking radio disable コマンドは、無線ベースのロケーションを無効にします。

undo rfid-tracking radio コマンドは、デフォルトに戻します。

AP がロケーションパケットをロケーションサーバに送信するには、AeroScout ロケーションと無線ベースのロケーションを両方有効にする必要があります。

例

AP ap1 で、無線ベースのロケーションを有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] rfid-tracking radio enable

AP グループ 1 の型番 QX-W1110 の AP で、無線ベースのロケーションを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] radio 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-radio-1] rfid-tracking radio enable

関連コマンド

rfid-tracking aeroscout

3.2 BLE機能の設定コマンド

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

3.2.1 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Module view

定義済みユーザロール

network-admin

パラメータ

text: モジュールの説明を指定します。text 引数は大文字と小文字を区別する 1～64 文字の文字列です。

説明

description コマンドはモジュールの説明を指定します。

undo description コマンドはモジュールの説明を削除します。

description コマンドでモジュールの説明を設定することが出来ます。

IoT AP にインストールまたは接続されているモジュールを効率的に管理するには、型番、場所、および機能に基づいたモジュールの説明を設定します。

例

#モジュール 1 の説明を L3-office に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] description L3-office

3.2.2 display wlan module-information

Syntax

display wlan module-information { all | ap *ap-name* **{ module all | module** *module-id* **} } [online]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての AP を指定します。

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

module all: すべてのモジュールを指定します。

module *module-id*: モジュール ID を指定します。*module-id* 引数の値の範囲は、AP モデルによって異なります。

online: オンライン状態のモジュールを指定します。

説明

display wlan module-information コマンドは AP のモジュール情報を表示します。

例

#AP ap1 のモジュール 1 に関する情報を表示します。

<AC> display wlan module-information ap ap1 module 1

```
AP name             :1110
Maximum modules      :1
  Module 1:
  Module administrative type    : BLE
  Module physical type         : NEC
  Model                       : T103-MP
  HW version                   : Ver.A
  SW version                   : A1253 V200R001B01D029SP53
  Serial ID                   : 219801A1LHA10A100626
  Module MAC                   : 0023-89e2-ed76
  Module physical status       : Normal
  Module administrative status  : Disabled
  Description                 : Not configured
```

表 3-2 コマンド出力

フィールド	説明
Module administrative type	設定されているモジュールタイプ
Module physical type	モジュールの物理タイプ
Model	モジュールの型番。使用可能なモジュールがない場合、このフィールドにはN/Aと表示されます。
HW version	モジュールのハードウェアバージョン

フィールド	説明
SW version	モジュールのソフトウェアバージョン
Serial ID	モジュールのシリアルID
Module MAC	モジュールのMACアドレス。（H-H-H形式）
Module physical status	物理モジュールの状態： • Unavailable • Normal • Absent
Module administrative status	モジュールの設定状態： • Enable • Disable
Description	モジュールの説明

3.2.3 display iot ble neighbor-information

Syntax

display iot ble neighbor-information ap *ap-name* **{ module all | module** *module-id* **| mac** *mac-addr* **}**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

module all: すべてのモジュールを指定します。

module *module-id*: モジュール ID を指定します。*module-id* 引数の値の範囲は、AP モデルによって異なります。

mac *mac-addr*: MAC アドレスを指定します。MAC アドレスは、大文字と小文字を区別しない XXXX-XXXX-XXXX 形式の 14 文字の文字列です。各 X は、0~9 の数字または a~f の小文字を表します。

説明

display iot ble neighbor-information コマンドは、AP 周辺の BLE デバイス情報を表示します。

例

#AP ap1 周辺の BLE デバイス情報を表示します。

<AC> display iot ble neighbor-information ap ap1 module 1

```
--------------------------------------------------------------------------------
--------
Module ID  MAC address     Address type         RSSI      Last update time
--------------------------------------------------------------------------------
--------
1          1111-2222-AAAA   Public               -5         Mon Nov  2 13:54:23
2021
1          ABAB-CCCC-FFFF   PrivateResolvable     6         Mon Nov  2 13:54:23
2021
```

表 3-3 コマンド出力

フィールド	説明
MAC address	BLEデバイスのMACアドレス
Address type	アドレスの種類： • Public • Static • PrivateResolvable • PrivateNonResolvable

3.2.4 iot auto-module

Syntax

iot auto-module { disable | enable }

undo iot auto-module

デフォルト

AP view: AP group view の設定を使用します。

AP group view: 無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

enable: 自動モジュール機能を有効にします。

disable: 自動モジュール機能を無効にします。

説明

iot auto-module enable コマンドは自動モジュール機能を有効にします。

iot auto-module disable コマンドは自動モジュール機能を無効にします。

undo iot auto-module コマンドはデフォルトに戻します。

自動モジュール機能を有効にすると、手動モジュールを設定しなくてもモジュールを AP に関連付けることができます。

AP view の設定は、AP group view の設定より優先されます。

例

#AP ap1 の自動モジュール機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] iot auto-module enable

#AP group 10 の自動モジュール機能を有効にします。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] iot auto-module enable

3.2.5 iot auto-module persistent

Syntax

iot auto-module persistent { disable | enable }

undo iot auto-module persistent

デフォルト

AP view: AP group view の設定を使用します。

AP group view: 無効

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

enable: 自動モジュール変換機能を有効にします。

disable: 自動モジュール変換機能を無効にします。

説明

iot auto-module persistent enable コマンドは自動モジュール変換機能を有効にします。

iot auto-module persistent disable コマンドは自動モジュール変換機能を無効にします。

undo iot auto-module persistent コマンドはデフォルトに戻します。

自動モジュール変換機能を有効にすると、モジュールがオンラインになった後、自動的に自動モジュールを手動モジュールに変換します。手動モジュールに自動的に変換されるのは、自動モジュール変換機能を有効にした後でオンラインになったモジュールのみです。オンライン状態の自動モジュールを手動モジュールに変換する場合は、**iot auto-module persistent all** コマンドを使用します。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 の自動モジュール変換機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] iot auto-module persistent enable

#AP group 10 の自動モジュール変換機能を有効にします。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] iot auto-module persistent enable

3.2.6 iot auto-module persistent all

Syntax

iot auto-module persistent all

View

AP view

AP group view

定義済みユーザロール

network-admin

説明

iot auto-module persistent all コマンドは、すべてのオンライン状態の自動モジュールを手動モジュールに変換し、変換された各モジュールにシリアル番号を自動的に割り当てます。

例

#AP ap1 のすべてのオンライン状態の自動モジュールを、手動モジュールに変換します。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] iot auto-module persistent all

#AP group 10 のすべてのオンライン状態の自動モジュールを、手動モジュールに変換します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] iot auto-module persistent all

3.2.7 module

Syntax

module *module-id*

View

AP view

AP group's AP model view

定義済みユーザロール

network-admin

パラメータ

module-id: モジュール ID を指定します。値の範囲は AP モデルによって異なります。

説明

module コマンドは module view に入ります。

例

#AP ap1 の module view に移行します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1]

#AP group apgroup10 の AP モデル QX-W1110 で、module view に移行します。

<AC> system-view

[AC] wlan ap-group apgroup1

[AC-wlan-ap-apgroup1] ap-model QX-W1110

[AC-wlan-ap-apgroup1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1]

3.2.8 module enable

Syntax

module { disable | enable }

undo module

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 無効

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

enable: モジュールを有効にします。

disable: モジュールを無効にします。

説明

module enable コマンドはモジュールを有効にします。

module disable コマンドはモジュールを無効にします。

undo module コマンドはデフォルトに戻します。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 のモジュールを有効にします。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] module enable

#AP group 1 の AP モデル QX-W1110 のモジュールを有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] module enable

3.2.9 module firmware-upgrade

Syntax

module firmware-upgrade { disable | enable }

undo module firmware-upgrade

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 有効

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

enable: モジュールの自動ファームウェアアップグレードを有効にします。

disable: モジュールの自動ファームウェアアップグレードを無効にします。

説明

module firmware-upgrade enable コマンドはモジュールの自動ファームウェアアップグレードを有効にします。

module firmware-upgrade disable コマンドはモジュールの自動ファームウェアアップグレードを無効にします。

undo module firmware-upgrade コマンドはデフォルトに戻します。

この機能により、ファームウェアバージョンが AP のイメージファイルに保存されているバージョンと異なる場合に、モジュールのファームウェアを自動でアップグレードできます。

モジュールに対してこの機能を有効にすると、モジュールがインストールされている IoT AP が再起動されるたびにこの機能が有効になります。

モジュールファームウェアのアップグレードプロセス中に、shutdown コマンドを使用して、ファームウェアアップグレード中の IoT AP と接続するインターフェイスをシャットダウンしないでください。Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 で module1 の、自動ファームウェアアップグレードを有効にします。

<AC> system-view

[AC] wlan ap ap1

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] module firmware-upgrade enable

#AP group 10 の AP モデル QX-W1110 で、module1 の自動ファームウェアアップグレードを有効にします。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] ap-model QX-W1110

[AClan-ap-group-10-ap-model-QX-W1110] module 1

[AClan-ap-group-10-ap-model-QX-W1110-module-1] module firmware-upgrade enable

3.2.10 rfid-tracking ble advertisement

Syntax

rfid-tracking ble advertisement [*ad-number* **] { major-id** *major-id* **| measured-power** *measured-power* **| minor-id** *minor-id* **| uuid** *uuid* **}**

undo rfid-tracking ble advertisement [*ad-number* **] { major-id | measured-power | minor-id | uuid }**

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: BLE モジュールの ad1 および ad2 のアドバタイズメント情報は、mjor-id は 1、minor-id は 1、measured-power は-58、uuid は E1CC5B618C06428E8720FE619DB80193 です。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

ad-number: アドバタイズメントタイプを指定します。この引数を指定しない場合、ad 1 アドバタイズメントが設定されます。

major-id *major-id*: BLE モジュールのアドバタイズメント情報の Major-ID を指定します。major-id 引数の値の範囲は 0 から 65535 です。

measured-power *measured-power*: BLE モジュールのアドバタイズメント情報の measured-power を指定します。*measured-power* 引数の値の範囲は 0~127 で、0〜-127 dBm の信号強度を表します。measured-power 引数の値が大きいほど信号強度が弱くなります。measured-power は、iBeacon を送信したデバイスから 1 m (3.28 フィート) 離して配置した、受信デバイスで検出される信号強度です。measured-power は、アドバタイズを受信したデバイスと iBeacon 送信デバイス間の距離の計算に使用できます。

minor-id *minor-id*: BLE モジュールのアドバタイズメント情報の Minor-ID を指定します。*minor-id* 引数の値の範囲は 0 から 65535 です。

uuid *uuid*: BLE モジュールのアドバタイズメント情報の uuid を指定します。*uuid* 引数の値の範囲は、大文字と小文字を区別しない 0~f の 32 桁の 16 進数文字列です。

説明

rfid-tracking ble advertisement コマンドは BLE モジュールのアドバタイズメント情報を設定します。

undo rfid-tracking ble advertisement コマンドはデフォルトに戻します。

BLE モジュールは、Major-ID、Minor-ID、Measured-power、UUID を含む iBeacon アドバタイズメントを近くのアプリケーションソフトウェアにブロードキャストします。アドバタイズメントを受信したアプリケーションソフトウェアは、アドバタイズメント情報に応じて特定の動作を行い、ソフトウェア機能を実現します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で、BLE module 1 の ad1 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement major-id 4

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement minor-id 4

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement uuid 34ae56115098ca67321a11256bca3007

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement measured-power 30

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の ad 1 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement major-id 4

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement minor-id 4

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement uuid 34ae56115098ca67321a11256bca3007

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement measured-power 30

#AP ap 1 上で、BLE モジュール 1 の ad 2 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 major-id 5

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 minor-id 5

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 uuid 44ae56115098ca67321a11256bca3008

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 measured-power 30

#AP グループ 1 の AP モデル QX-W 1110 で、BLE モジュール 1 の ad 2 アドバタイズメント情報を設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 major-id 5

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 minor-id 5

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 uuid 44ae56115098ca67321a11256bca3008

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 measured-power 30

3.2.11 rfid-tracking ble advertisement { disable | enable }

Syntax

rfid-tracking ble advertisement { disable | enable }

undo rfid-tracking ble advertisement

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 無効

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

enable: BLE モジュールの iBeacon 送信機能を有効にします。

disable: BLE モジュールの iBeacon 送信機能を無効にします。

説明

rfid-tracking ble advertisement enable コマンドは BLE モジュールの iBeacon 送信機能を有効にします。

rfid-tracking ble advertisement disable コマンドは BLE モジュールの iBeacon 送信機能を無効にします。

undo rfid-tracking ble advertisement コマンドはデフォルトに戻します。

BLE モジュールが iBeacon ad1 および ad2 アドバタイズメントを定期的にブロードキャストできるようにします。iBeacon アドバタイズメントには、UUID、Major-ID、Minor-ID が含まれます。ad1 または ad2 アドバタイズメントのパラメータを設定するには、rfid-tracking ble advertisement コマンドを使用します。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap 1 上の BLE モジュール 1 の iBeacon 送信機能を有効にします。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement enable

#AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の iBeacon 送信機能を有効にします。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement enable

3.2.12 rfid-tracking ble advertisement interval

Syntax

rfid-tracking ble advertisement [*ad-number* **] interval** *interval*

undo rfid-tracking ble advertisement [*ad-number* **] interval**

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: BLE モジュールの iBeacon ad1 および ad2 アドバタイズメントをブロードキャストする間隔は 100 センチ秒です。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

ad-number: アドバタイズメントタイプを指定します。この引数を指定しない場合、コマンドは ad1 アドバタイズメントをブロードキャストする間隔を設定します。

interval: BLE モジュールが iBeacon アドバタイズメントをブロードキャストする間隔を 10 の倍数値で指定します。値の範囲は 50~1000 で、単位はセンチ秒です。

説明

rfid-tracking ble advertisement interval コマンドは BLE モジュールが iBeacon をブロードキャストする間隔を設定します。

undo rfid-tracking ble advertisement interval コマンドはデフォルトに戻します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で、BLE module 1 の ad1 アドバタイズメントを 200 センチ秒ごとにブロードキャストするように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement interval 200

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の ad 1 アドバタイズメント情報を 200 センチ秒ごとにブロードキャストするように設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement interval 200

#AP ap 1 上で、BLE モジュール 1 の ad 2 アドバタイズメント情報を 200 センチ秒ごとにブロードキャストするように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement ad2 interval 200

#AP グループ 1 の AP モデル QX-W 1110 で、BLE モジュール 1 の ad 2 アドバタイズメント情報を 200 センチ秒ごとにブロードキャストするように設定します

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement ad2 interval 200

3.2.13 rfid-tracking ble advertisement mode

Syntax

rfid-tracking ble advertisement mode { continuous *ad-number* **| periodic {** *ad-number period* **}&<***2***> }**

undo rfid-tracking ble advertisement mode

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: BLE モジュールの iBeacon ad1 のアドバタイズメントを連続モードで送信します。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

continuous: 連続モードを指定します。

ad-number: アドバタイズメントタイプを指定します。

periodic: *Periodic モードを指定します。*

{ ad-number period }&<2>: アドバタイズメントタイプとアドバタイズメント期間を 10 の倍数値で指定します。アドバタイズメント期間の範囲は 50～6000 で、単位はセンチ秒

です。&<2>は、2 つのアドバタイズメントタイプと 2 つのアドバタイズメント期間を指定する必要があることを示します。

説明

rfid-tracking ble advertisement mode コマンドは BLE アドバタイズメントモードを設定します。

undo rfid-tracking ble advertisement mode コマンドはデフォルトに戻します。

BLE モジュールは、次のモードでアドバタイズメントを送信できます。

- 連続モード: 指定された間隔で 1 種類のアドバタイズメント (ad 1 または ad 2) だけを送信します。
- Periodic モード: 指定した間隔で ad 1 アドバタイズメントと ad 2 アドバタイズメントを交互に送信します。

たとえば、ad1 アドバタイズメント期間が 210 センチ秒、ad2 アドバタイズメント期間が 310 センチ秒、アドバタイズメント間隔がそれぞれ 100 センチ秒の場合、BLE モジュールは、最初に 210 センチ秒の間に 3 つの ad 1 アドバタイズメントを送信し、次に 310 センチ秒の間に 4 つの ad2 アドバタイズメントを送信します。このパターンでは、BLE モジュールは ad1 および ad2 アドバタイズメントを交互に送信します。

アドバタイズメント間隔は、rfid-tracking ble advertisement interval コマンドを使用して設定します。

Module view の設定は、AP group module view の設定より優先されます。

例

AP ap1 で、BLE module 1 の ad1 アドバタイズメントを連続モードで送信するように設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement mode continuous ad1

AP グループ 1 の AP モデル QX-W 1110 で、BLE module 1 の ad 1 アドバタイズメント情報を連続モードで送信するように設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement mode continuous ad1

#AP ap 1 上で、BLE モジュール 1 の ad1 および ad2 のアドバタイズメント情報を Periodic モードで送信するように設定します。ad1 のアドバタイズメント期間を 200 センチ秒、ad2 のアドバタイズメント期間を 100 センチ秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement mode periodic ad1 200 ad2 100

#AP グループ 1 の AP モデル QX-W 1110 で、BLE モジュール 1 の ad1 および ad2 のアドバタイズメント情報を Periodic モードで送信するように設定します。ad1 のアドバタイズメント期間を 200 センチ秒、ad2 のアドバタイズメント期間を 100 センチ秒に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] rfid-tracking ble advertisement mode periodic ad1 200 ad2 100

3.2.14 rfid-tracking ble aging-time

Syntax

rfid-tracking ble aging-time *aging-time*

undo rfid-tracking ble aging-time

デフォルト

AP view: AP group view の設定を使用します。AP group view に設定がない場合、global configuration view の設定を使用します。

AP group view: global configuration view の設定を使用します。

global configuration view: 180 秒

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

aging-time: エージングタイムを 60~3600 秒の範囲で指定します

説明

rfid-tracking ble aging-time コマンドは BLE デバイスのエージングタイムを設定します。

undo rfid-tracking ble aging-time コマンドはデフォルトに戻します。

rfid-tracking ble aging-time コマンドは、BLE デバイスのエージングタイムを設定します。AP view の設定は、AP group view の設定よりも優先されます。AP group view の設定は、グローバル設定 view の設定よりも優先されます

例

#AP ap 1 の BLE デバイスのエージングタイムを 60 秒に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] rfid-tracking ble aging-time 60

#AP group 10 の BLE デバイスのエージングタイムを 60 秒に設定します。

<AC> system-view

[AC] wlan ap-group 10

[AC-wlan-ap-group-10] rfid-tracking ble aging-time 60

#BLE デバイスのエージングタイムをグローバルで 60 秒に設定します。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] rfid-tracking ble aging-time 60

3.2.15 tx-power

Syntax

tx-power { *power-level* **| value** *power-value* **}**

undo tx-power

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 送信電力レベル 1 です。これは送信電力 4dBm を示します。

View

Module view

AP group module view

定義済みユーザロール

network-admin

パラメータ

power-level:送信電力レベルを指定します。値は 1、2、3、4 のいずれかで、それぞれ 4 dBm、-1 dBm、-5 dBm、-9 dBm の送信電力を示します。

value *power-value*: 送信電力を指定します。値の範囲は-40 dBm~+8 dBm です。

説明

tx-power コマンドはモジュールの送信電力を設定します。

undo tx-power コマンドはデフォルトに戻します。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 のモジュール 1 の送信電力レベルを 4 に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] tx-power 4

#AP group 1 の AP モデル QX-W1110 で、モジュール 1 の送信電力レベルを 4 に設定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] tx-power 4

3.2.16 type ble

Syntax

type ble

undo type

デフォルト

Module view: AP group module view の設定を使用します。

AP group module view: 設定なし

View

Module view

AP group module view

定義済みユーザロール

network-admin

説明

type ble コマンドは、サポート対象モジュールタイプとして BLE を指定します。

undo type コマンドはデフォルトに戻します。

AP 上のモジュールが正しく動作するには、指定するサポート対象モジュールタイプが物理モジュールタイプと一致している必要があります。

Module view の設定は、AP group module view の設定より優先されます。

例

#AP ap1 のモジュール 1 でサポート対象モジュールタイプとして BLE を指定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1110

[AC-wlan-ap-ap1] module 1

[AC-wlan-ap-ap1-module-1] type ble

#AP group 1 の AP モデル QX-W1110 で、モジュール 1 のサポート対象モジュールとして BLE を指定します。

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1110

[AC-wlan-ap-group-1-ap-model-QX-W1110] module 1

[AC-wlan-ap-group-1-ap-model-QX-W1110-module-1] type ble

3.2.17 wlan execute module reset

Syntax

wlan execute module reset ap *ap-name* **module** *module-id*

View

System view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*: AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む、大文字と小文字を区別する 1～64 文字の文字列です。

module *module-id*: モジュール ID を指定します。module-id 引数の値の範囲は、AP モデルによって異なります。

説明

wlan execute module reset コマンドは AP のモジュールを再起動します。

例

#AP ap1 のモジュール 1 を再起動します。

<AC> system-view

[AC] wlan execute module reset ap ap1 module 1

3.3 サーバへのIoTデータのレポート設定コマンド

🕮 **メモ：**

この章のコマンドは、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

3.3.1 azure-dps group-symmetric-key

Syntax

azure-dps group-symmetric-key { cipher | simple } *string*

undo azure-dps group-symmetric-key

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号テキストで鍵を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、平文形式で指定された鍵は暗号化された形式で保存されます。

string: 鍵の文字列を指定します。暗号テキストの鍵は大文字と小文字を区別する 33～201 の文字列です。プレーンテキストの鍵は大文字と小文字を区別する 1～128 文字の文字列です。

説明

azure-dps group-symmetric-key コマンドは Microsoft Azure IoT Hub DPS のグループ対称キーを設定します。

undo azure-dps group-symmetric-key コマンドはデフォルトに戻します。

IoT データレポート用のサーバが Microsoft Azure IoT hub DPS の場合、IoT トランスポートプロファイルを有効にする前に、このコマンドを実行する必要があります。グループ対称キーを編集する場合、事前に IoT トランスポートプロファイルを無効にする必要があります。

例

#Microsoft Azure IoT hub DPS のグループ対称キーを、暗号テキストで設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] azure-dps group-symmetric-key cipher OpsBHTTubGabpHTmYbc3w7dKqG9XC6e8OS2apbHRMtVunBkYTY9B/ScyjLeRpf7cjJxXPIsIqna8WV1DePS8uA==

関連コマンド

iot transport-profile

3.3.2 azure-dps id-scope

Syntax

azure-dps id-scope *id-scope*

undo azure-dps *id-scope*

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

id-scope: Microsoft Azure IoT Hub DPS の ID スコープの文字列を指定します。ID スコープは 1～63 文字の文字列です。

説明

azure-dps id-scope コマンドは Microsoft Azure IoT Hub DPS の ID スコープを設定します。

undo azure-dps id-scope コマンドはデフォルトに戻します。

IoT データレポート用のサーバが Microsoft Azure IoT hub DPS の場合、IoT トランスポートプロファイルを有効にする前に、このコマンドを実行する必要があります。ID スコープを編集する場合、事前に IoT トランスポートプロファイルを無効にする必要があります。

例

#Microsoft Azure IoT hub DPS の ID スコープを 1234567890a として設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] azure-dps id-scope 1234567890a

関連コマンド

iot transport-profile

3.3.3 display iot transport-profile

Syntax

display iot transport-profile

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display iot transport-profile コマンドは、IoT トランスポートプロファイルに関する情報を表示します。

IoT トランスポートプロファイルに関する情報を表示するには、まず System view で IoT トランスポートプロファイルを作成する必要があります。

例

#作成されたすべての IoT トランスポートプロファイルに関する情報を表示します。

<AC> display iot transport-profile

```
Profile name                Server type          Status
Azureiot1                   Azure                Enabled
Azureiot2                   Azure                Disabled
```

表 3-4 コマンド出力

フィールド	説明
Server type	サーバタイプ。サポートされているのはAzureのみ。
Status	IoTトランスポートプロファイルの状態: • Enabled • Disabled

関連コマンド

iot-transport-profile

3.3.4 display iot transport-profile in-use

Syntax

display iot transport-profile in-use

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display iot transport-profile in-use コマンドは、使用中の IoT トランスポートプロファイルに関する情報を表示します。

例

#使用中の IoT トランスポートプロファイルに関する情報を表示します。

<AC> display iot transport-profile in-use

```
Connect status: connected
Connected for: 0d 19h 20m 15s
Profile name: aaa
```

```
Server URL: global.azure-devices-provisioning.net
Server type: azure iot
Azure DPS information:
  ID scope: 0cn0002B978
  Key type: symmetric
  Group                                                    key(cipher):
$c$3$hQpNztebohdFlXL5p0aVIsA4Hn2QYH5PIWSJDTtZr0mwKW942Erghtscx0aZ3
osazfgmTSZ0PKjz5DavZFpYk6y/ijJqAHC5U+6jIltCjhh2vrRCsh2gNiCnHGpOEr8YH0HJhHOzxE
acd6Q=
  Register ID: sn-210235A3KYC187000028
Report interval: 60 seconds
Keepalive interval: 60 seconds
Total sent messages: 0
Sent BLE data messages: 0
Sent keepalive messages: 0
Total received messages: 0
```

表 3-5 コマンド出力

フィールド	説明
Connect status	デバイスとサーバ間の接続の状態: ● connecting－接続試行中 ● connected －接続 ● disconnected－切断
Connected for	サーバとの接続時間
Profile name	IoTトランスポートプロファイル名
Server URL	サーバのURL
Server type	サービスタイプ。現在のソフトウェアではMicrosoft Azure IoT Hub DPSのみをサポートしています。
Azure DPS information	Azure DPSの情報
ID scope	Azure DPSのIDスコープ。
Key type	Azure DPSキーの種類。現在のソフトウェアでは対称キーのみをサポートしています。
Group key(cipher)	Azure DPS登録グループの対称キー。キーは暗号テキストで表示されます。
Register ID	Azure DPSのデバイス登録ID

フィールド	説明
Report interval	APがIoTデータをサーバにレポートする間隔。単位は秒です。
Keepalive interval	サーバにキープアライブパケットを送信する間隔。単位は秒です。
Total sent messages	送信したメッセージの合計数
Sent BLE data messages	送信したBLEデータメッセージの合計数
Sent keepalive messages	送信したキープアライブメッセージの合計数
Total received messages	受信したメッセージの合計数

3.3.5 iot transport-profile

Syntax

iot transport-profile *transport-profile-name*

undo iot transport-profile *transport-profile-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

transport-profile-name: IoT トランスポートプロファイル名を指定します。IoT トランスポートプロファイル名は、大文字、小文字を区別しない 1～63 文字の文字列です。

説明

iot transport-profile コマンドは IoT トランスポートプロファイルを作成し、その View に入るか、既存の IoT トランスポートプロファイル View に入ります。

undo iot transport-profile コマンドは IoT トランスポートプロファイルを削除します。

IoT トランスポートプロファイルには、IoT データを送信する宛先のサーバアドレスや、レポート間隔などを設定します。

IoT トランスポートプロファイルは最大 8 個まで作成できます。

IoT トランスポートプロファイルを削除する場合、事前に IoT トランスポートプロファイルのバインド設定を解除する必要があります。

例

#IoT トランスポートプロファイル azureiothub を作成し、その view に移行します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub]

関連コマンド

iot-transport-profile

3.3.6 iot-transport-profile

Syntax

iot-transport-profile *transport-profile-name*

undo iot-transport-profile *transport-profile-name*

デフォルト

設定なし

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

transport-profile-name: IoT トランスポートプロファイル名を指定します。IoT トランスポートプロファイル名は、大文字と小文字は区別しない 1～63 文字の文字列です。

説明

iot-transport-profile コマンドは IoT トランスポートプロファイルをバインドします。

undo iot-transport-profile コマンドはデフォルトに戻します。

オンライン AP は、グローバルコンフィグレーション view で IoT トランスポートプロファイルをバインドした後にのみ、IoT データをサーバにレポートします。

既存の IoT トランスポートプロファイル名のみを指定できます。

このコマンドを複数回実行した場合、最新の設定が有効になります。

例

#グローバルコンフィグレーション view で、IoT トランスポートプロファイル azureiothub をバインドします。

<AC> system-view

[AC] wlan global-configuration

[AC-wlan-global-configuration] iot-transport-profile azureiothub

関連コマンド

iot transport-profile

3.3.7 keepalive interval

Syntax

keepalive interval *interval*

undo keepalive interval

デフォルト

60 秒

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

interval: キープアライブパケットを送信する間隔を 1~600 秒の範囲で指定します。

説明

keepalive interval コマンドは装置がサーバにキープアライブパケットを送信する間隔を設定します。

undo keepalive interval コマンドはデフォルトに戻します。

例

#キープアライブパケットを 50 秒毎にサーバに送信するように設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] keepalive interval 50

関連コマンド

iot transport-profile

3.3.8 report interval

Syntax

report interval *interval*

undo report interval

デフォルト

60 秒

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

interval: IoT データをサーバにレポートする間隔を 1~600 秒の範囲で指定します。

説明

report interval コマンドは IoT データをサーバにレポートする間隔を設定します。

undo report interval コマンドはデフォルトに戻します。

レポートする間隔が長すぎるとサービスに影響しますが、間隔を短くすると AC の負荷が増加するため、適切な値を設定する必要があります。

例

#50 秒毎に IoT データをサーバにレポートするように設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] report interval 50

関連コマンド

iot transport-profile

3.3.9 server-url

Syntax

server-url *server-url-string*

undo server-url

デフォルト

設定なし

View

IoT transport profile view

定義済みユーザロール

network-admin

パラメータ

server-url-string: サーバの URL を指定します。サーバの URL は、大文字と小文字を区別する 1～127 文字の文字列です。

説明

server-url コマンドは IoT データレポート用のサーバの URL を設定します。

undo server-url コマンドはデフォルトに戻します。

IoT トランスポートプロファイルを有効にする前に、このコマンドを設定する必要があります。

サーバの URL を編集する場合、事前に IoT トランスポートプロファイルを無効にする必要があります。

このコマンドを複数回実行した場合は、最新の設定が有効になります。

例

#IoT データレポート用のサーバの URL を global.azure-devices-provisioning.net として設定します。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] server-url global.azure-devices-provisioning.net

関連コマンド

iot transport-profile

3.3.10 transport-profile enable

Syntax

transport-profile enable

undo transport-profile enable

デフォルト

無効

View

IoT transport profile view

定義済みユーザロール

network-admin

説明

transport-profile enable コマンドは IoT トランスポートプロファイルを有効にします。

undo transport-profile enable コマンドはデフォルトに戻します。

例

#IoT トランスポートプロファイル azureiothub を有効にします。

<AC> system-view

[AC] iot transport-profile azureiothub

[AC-iot-tp-azureiothub] transport-profile enable

関連コマンド

iot transport-profile

目次

このセクションのページは **12-x-x** です。

4 章 Hotspot 2.0 の設定 4-1
4.1 Hotspot 2.0 の設定コマンド 4-1
4.1.1 3gpp-info 4-1
4.1.2 authentication-type 4-2
4.1.3 comeback-delay 4-3
4.1.4 description 4-3
4.1.5 dgaf enable 4-4
4.1.6 display wlan hotspot uploaded-osu-icon 4-5
4.1.7 domain-name 4-6
4.1.8 friendly-name 4-7
4.1.9 gas-limit 4-8
4.1.10 hessid 4-8
4.1.11 hotspot-policy 4-9
4.1.12 icon-file 4-10
4.1.13 ip-protocol 4-12
4.1.14 ip-type 4-13
4.1.15 method 4-14
4.1.16 nai 4-15
4.1.17 nai-realm 4-16
4.1.18 network-type 4-18
4.1.19 operator-name 4-20
4.1.20 osu-provider 4-20
4.1.21 osu-ssid 4-22
4.1.22 policy-name 4-22
4.1.23 roam-oi 4-23
4.1.24 uri 4-24
4.1.25 venue group 4-25
4.1.26 venue name 4-28
4.1.27 wan-metrics 4-29
4.1.28 wlan hotspot-policy 4-30
4.1.29 wlan hotspot osu-icon unload 4-31
4.1.30 wlan hotspot osu-icon upload 4-32
4.1.31 wlan osu-provider 4-33
4.1.32 wlan venue url-unescape-chars 4-33

4章 Hotspot 2.0 の設定

🕮 **メモ：**

Hotspot 2.0 の設定は、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

4.1 Hotspot 2.0の設定コマンド

4.1.1 3gpp-info

Syntax

3gpp-info country-code *mobile-country-code* **network-code** *mobile-network-code*

undo 3gpp-info country-code *mobile-country-code* **network-code**

mobile-network-code

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

mobile-country-code: モバイル国コード(MCC)を指定します。MCC は、クライアントが属する国を一意に識別する 3 桁の数値コードです。

mobile-network-code: モバイルネットワークコード(MNC)を指定します。モバイルネットワークコードは、クライアントが属するモバイルネットワークを一意に識別する 2 桁または 3 桁の数値コードです。

説明

3gpp-info コマンドは 3GPP 情報を設定します。

undo 3gpp-info コマンドは 3GPP 情報を削除します。

Hotspot 2.0 ポリシーでは、最大 32 個の国コードとモバイルネットワークコードの組み合わせを指定できます。

1 つの国コードを複数のモバイルネットワークコードと組み合わせることができます。

例

3GPP 情報を設定するため、国コードを 460 に、ネットワークコードを 01 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] 3gpp-info country-code 460 network-code 01

4.1.2 authentication-type

Syntax

authentication-type { **0** [**redirect-url** *url*] | **1** | **2 redirect-url** *url* | **3** }

undo authentication-type { **0** | **1** | **2** | **3** }

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

0: 使用条件への同意を指定します。

1: オンライン登録を指定します。

2: HTTP/HTTPS リダイレクトを指定します。

3: DNS リダイレクトを指定します。

redirect-url *url*: リダイレクトされた URL アドレスを指定します。

説明

authentication-type コマンドはネットワーク認証の種類を指定します。

undo authentication-type コマンドはネットワーク認証の種類を削除します。

Hotspot 2.0 ポリシーには、最大 4 つのネットワーク認証タイプを指定できます。

例

ネットワーク認証タイプを指定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] authentication-type 1

4.1.3 comeback-delay

Syntax

comeback-delay *value*

undo comeback-delay

デフォルト

1 TU

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

value: カムバック遅延を 1 から 1024 TU の範囲で指定します。1TU は 1024 μs に相当します。

説明

comeback-delay コマンドはクライアントが GAS カムバック要求を送信するためのカムバック遅延を設定します。

undo comeback-delay コマンドはデフォルトを復元します。

クライアントが多くの GAS カムバック要求を送信するのを防ぐことができます。

例

カムバック遅延を 10 TU に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] comeback-delay 10

4.1.4 description

Syntax

description *description* **lang-code** *lang-code*

undo description *description* **lang-code** *lang-code*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

description: 説明を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 言語コードを指定します。デバイスは、一般的な国際標準をサポートします。

説明

description コマンドは OSU サーバの説明を設定します。

undo description コマンドは OSU サーバの説明を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

OSU サーバには、最大 32 個の説明を設定できます。クライアントには、クライアントシステムと同じ言語の説明が 1 つ表示されます。

例

OSU サーバ 1 の説明を設定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] description "Free service for test purpose" lang-code eng

4.1.5 dgaf enable

Syntax

dgaf enable

undo dgaf enable

デフォルト

有効

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

説明

dgaf enable コマンドは Downstream Group-Addressed Forwarding(DGAF)を有効にします。

undo dgaf enable コマンドは DGAF を無効にします。

DGAF を使用すると、AP はすべてのダウンストリームワイヤレスブロードキャスト ARP パケットおよびワイヤレスマルチキャストパケットを転送できます。ダウンストリームマルチキャストを使用したスプーフィング攻撃を防止するには、AP の DGAF を無効にします。

DGAF を無効にする前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認します。

パケット損失を回避するには、DGAF を無効にする前にプロキシ ARP とマルチキャスト最適化を有効にします。プロキシ ARP の詳細については、オペレーションマニュアルのセクション 5 *ネットワーク接続*“*Proxy ARP*”を参照してください。

例

DGAF を無効にします。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] undo dgaf enable

4.1.6 display wlan hotspot uploaded-osu-icon

Syntax

display wlan hotspot uploaded-osu-icon

View

Any view

定義済みユーザロール

network-admin

network-operator

説明

display wlan hotspot uploaded-osu-icon コマンドはアップロードされた OSU サーバアイコンのリストを表示します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

例

アップロードされた OSU サーバアイコンのリストを表示します。

<AC> display wlan hotspot uploaded-osu-icon

```
Total uploaded osu icon count: 1
Icon name                       Icon type
--------------------------------------------------------------------------------
college.png                     png
```

関連コマンド

- **icon-file**
- **wlan hotspot osu-icon upload**

4.1.7 domain-name

Syntax

domain-name *domain-name*

undo domain-name *domain-name*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名を指定します。大文字と小文字が区別される 1 から 255 文字の文字列です。

説明

domain-name コマンドはドメイン名を設定します。

undo domain-name コマンドはドメイン名を削除します。

1 つの Hotspot 2.0 ポリシーでは、最大 32 個のドメイン名を設定できます。

例

Hotspot 2.0 ポリシー1 でドメイン名を college に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] domain-name college

4.1.8 friendly-name

Syntax

friendly-name *friendly-name* **lang-code** *lang-code*

undo friendly-name *friendly-name* **lang-code** *lang-code*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

description: 説明を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 言語コードを指定します。デバイスは、一般的な国際標準をサポートします。

説明

friendly-name コマンドは OSU サーバの名前を設定します。

undo friendly-name コマンドは指定した OSU サーバ名を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。OSU サーバには最大 32 個の名前を設定できます。クライアントには、クライアントシステムと同じ言語の名前が表示されます。

OSU サーバがすでに Hotspot 2.0 ポリシーにバインドされている場合、サーバに指定された最新の名前を削除することはできません。

例

OSU サーバ 1 の名前を設定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] friendly-name osu1 lang-code en

4.1.9 gas-limit

Syntax

gas-limit number *number* **interval** *interval*

undo gas-limit

デフォルト

AC が受信できる GAS 初期要求の数に制限はありません。

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

number *number*: AC が受信できる GAS 初期要求の最大数を 10 から 60 の範囲で指定します。

Interval *interval*: AC が GAS 初期要求を受信する間隔を 10 から 60 秒の範囲で指定します。

説明

gas-limit コマンドは AC が指定された間隔内に受信できる GAS 初期要求の最大数を設定します。

undo gas-limit コマンドはデフォルトを復元します。

AC が受信した GAS 初期要求の数が制限を超えた場合、超過したフレームは廃棄されます。

例

AC が 15 秒以内に受信できる GAS 初期要求の最大数を 50 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] gas-limit number 50 interval 15

4.1.10 hessid

Syntax

hessid *hessid*

undo hessid

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

hessid: 同一 ESS を一意に識別する HESSID を H-H-H 形式で指定します。値をすべてゼロにすることはできません。

説明

hessid コマンドは同一 ESS 識別子(HESSID)を設定します。

undo hessid コマンドはデフォルトを復元します。

HESSID を設定する前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認してください。

例

Hotspot 2.0 ポリシー1 で HESSID を 0000-5e00-5310 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] hessid 0000-5e00-5310

4.1.11 hotspot-policy

Syntax

hotspot-policy *policy-number*

undo hotspot-policy

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

policy-number: Hotspot 2.0 ポリシーの番号を 1 から 32 の範囲で指定します。

説明

hotspot-policy コマンドは Hotspot 2.0 ポリシーをサービステンプレートにバインドします。

undo hotspot-policy コマンドはデフォルトに戻します。

Hotspot 2.0 ポリシーをサービステンプレートにバインドする場合は、次のガイドラインに従ってください。

- Hotspot 2.0 ポリシーが存在し、サービステンプレートが無効になっていることを確認してください。
- サービステンプレートが次のように設定されていることを確認してください。
  - 802.1X 認証および鍵管理モード
  - RSN IE
  - AES-CCMP 暗号スイート

例

Hotspot 2.0 ポリシー1 をサービステンプレート 1 にバインドします。

<AC> system-view

[AC] wlan service-template 1

[AC-wlan-st-1] hotspot-policy 1

4.1.12 icon-file

Syntax

icon-file *filename* **lang-code** *lang-code* **icon-type** *icon-type*

undo icon-file *filename*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

filename: アイコンファイルを名前で指定します。1 から 63 文字の文字列で、大文字と小文字が区別されます。

lang-code *lang-code*: 言語コードを指定します。デバイスは、一般的な国際標準をサポートしています。

icon-type *icon-type*: アイコンファイルの種類を指定します。1 から 15 文字の文字列で、大文字と小文字が区別されます。

説明

icon-file コマンドは OSU サーバのアイコンを指定します。

undo icon-file コマンドは OSU サーバの指定したアイコンを削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

コマンドが実行されると、デバイスは指定されたアイコンを読み込みます。OSU サーバには最大 6 つのアイコンを指定できます。クライアントには、クライアントシステムと同じ言語のアイコンが表示されます。

OSU サーバのアイコンを指定する場合は、次の制限とガイドラインに従ってください。

- バージョンファイルが保存されているルートディレクトリに icon という名前のディレクトリを作成し、FTP または TFTP を使用してアイコンファイルをフォルダにダウンロードしてからコマンドを実行します。
- 指定したアイコンファイルがアイコンディレクトリにない場合、アイコンファイルを読み込めません。アイコンファイルを読み込むには、アイコンディレクトリにアイコンファイルを保存してから、**wlan hotspot osu-icon upload** コマンドを実行してください。
- ファイルサイズは 64 KB を超えることはできません。
- コマンドで指定されたファイルの種類が実際のファイルの種類と同じであることを確認してください。
- OSU サーバがすでに Hotspot 2.0 ポリシーにバインドされている場合、最後に指定した OSU サーバのアイコンを削除することはできません。

例

OSU サーバ 1 のアイコンを指定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] icon-file test_icon lang-code eng icon-type png

4.1.13 ip-protocol

Syntax

ip-protocol { **esp** | **icmp** | **tcp** | **udp** } **port-number** *port-number* { **closed** | **open** | **unknown** }

undo ip-protocol { **esp** | **icmp** | **tcp** | **udp** } **port-number** *port-number*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

esp: ESP プロトコルを指定します。

icmp: ICMP プロトコルを指定します。

tcp: TCP プロトコルを指定します。

udp: UDP プロトコルを指定します。

port-number: ポート番号を指定します。

表 4-1 ポート番号とプロトコル種別

プロトコル種別	ポート番号	説明
ICMP	0	診断で使用されます。
TCP	20	FTPで使用されます。
TCP	22	SSHで使用されます。
TCP	80	HTTPで使用されます。
TCP	443	TLS VPNで使用されます。
TCP	1723	Point to Point Tunneling Protocol VPNで使用されます。
TCP	5060	VoIPで使用されます。
UDP	500	IKEv2(IPSec VPN)で使用されます。
UDP	5060	VoIPで使用されます。
UDP	4500	IKEv2(IPSec VPN)で使用されます。
ESP	0	IPSec VPNで使用されます。

closed: ポートステータスをクローズとして指定します。

open: ポートステータスをオープンとして指定します。

unknown: ポートステータスを不明として指定します。

説明

ip-protocol コマンドは IP プロトコルのポートステータスを設定します。

undo ip-protocol コマンドは設定を削除します。

例

ポート番号を 20 に設定し、TCP のポートステータスをオープンに設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] ip-protocol tcp port-number 20 open

4.1.14 ip-type

🕮 **メモ：**

IPv6 は未サポートです。

Syntax

ip-type ipv4 *ipv4-type* **ipv6** *ipv6-type*

undo ip-type

デフォルト

可用性は、IPv4 アドレスの場合は 1、IPv6 アドレスの場合は 2 です。

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

ipv4-type: IPv4 アドレスの可用性を 0～7 の範囲で指定します。

表 4-2 IPv4 アドレスの可用性

アドレス値	説明
0	アドレスの種類は使用できません。
1	使用可能なパブリックIPv4アドレスです。

アドレス値	説明
2	使用可能なポート制限IPv4アドレスです。
3	使用可能な単一NATプライベートIPv4アドレスです。
4	使用可能なダブルNATプライベートIPv4アドレスです。
5	使用可能なポート制限付きIPv4アドレスおよび単一NAT IPv4アドレスです。
6	使用可能なポート制限付きIPv4アドレスおよびダブルNAT IPv4アドレスです。
7	アドレスタイプの可用性が不明です。

ipv6-type: IPv6 アドレスの可用性を 0～2 の範囲で指定します。

表 4-3 IPv6 アドレスの可用性

アドレス値	説明
0	アドレスの種類は使用できません。
1	使用可能なアドレスタイプです。
2	アドレスタイプの可用性が不明です。

説明

ip-type コマンドは IP アドレスの可用性を設定します。

undo ip-type コマンドはデフォルトに戻します。

例

可用性を IPv4 アドレスの場合は 2、IPv6 アドレスの場合は 1 に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] ip-type ipv4 2 ipv6 1

4.1.15 method

Syntax

method *method-id*

undo method *method-id*

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

method-id: プロトコル ID を指定します。

- 0: OMA-DM を指定します。
- 1: SOAP-XML SPP を指定します。

説明

method コマンドはクライアントが OSU サーバと通信するためのプロトコルを指定します。

undo method コマンドはクライアントが OSU サーバと通信するための指定されたプロトコルを削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

両方のプロトコルを指定できます。クライアントは、OSU サーバと通信するためのプロトコルを選択します。

OSU サーバが既に Hotspot 2.0 ポリシーにバインドされている場合は、クライアントが OSU サーバと通信するために指定された最新のプロトコルを削除することはできません。

例

クライアントが OSU サーバと通信するためのプロトコルを指定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] method 0

4.1.16 nai

Syntax

nai *nai*

undo nai

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

nai: NAI を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

説明

nai コマンドは OSU サーバのネットワークアクセス識別子(NAI)を設定します。

undo nai コマンドは OSU サーバに設定した NAI を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

OSU サーバに対して NAI が設定されている場合、クライアントは OSEN OSU を介して OSU AP に接続します。OSU サーバに対して NAI が設定されていない場合、クライアントは Open OSU を介して OSU AP に接続します。

例

OSU サーバ 1 の NAI を設定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] nai abc@example.com

4.1.17 nai-realm

Syntax

nai-realm name *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* **authentication** *authentication*

undo nai-realm name *realm-name* [**eap-method** *eap-method-id* [**auth-method** *auth-method-id* [**authentication** *authentication*]]]

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

name *realm-name*: NAI レルム名を指定します。1 から 255 文字の文字列で、大文字と小文字が区別されます。

eap-method *eap-method-id*: EAP 認証方式を ID で指定します。

表 4-4 EAP 認証方式

eap-method-id	説明
1	EAP-Transport Layer Security (EAP-TLS)
2	Lightweight Extensible Authentication Protocol (LEAP)
3	EAP for GSM Subscriber Identity Module (EAP-SIM)
4	EAP-Tunneled Transport Layer Security (EAP-TTLS)
5	EAP-Authentication and Key Agreement (EAP-AKA)
6	Protected EAP (PEAP)

auth-method *auth-method-id*: 認証方式を ID で指定します。

authentication *authentication*: 認証パラメータを ID で指定します。

表 4-5 認証方式および認証パラメータ

auth-method-id	auth-method-type	authentication
2	Non-EAP Inner Authentication Type	• 1: PAP • 2: CHAP • 3: MSCHAP • 4: MSCHAPV2
5	Credential Type	• 1: SIM • 2: USIM • 3: NFC Secure Element • 4: Hardware Token • 5: Soft Token • 6: Certificate • 7: username/password • 8: none

auth-method-id	auth-method-type	authentication
6	Tunneled EAP Method Credential Type	• 1: SIM • 2: USIM • 3: NFC Secure Element • 4: Hardware Token • 5: Soft Token • 6: Certificate • 7: username/password • 8: Reserved • 9: Anonymous

説明

nai-realm コマンドは NAI レルムを作成し、NAI レルムの認証タイプを指定します。

undo nai-realm コマンドは NAI レルムを削除します。

undo nai-realm コマンドを使用する場合は、次のガイドラインに従ってください。

- **undo nai-realm name** *realm-name* コマンドは、同じ名前を使用するすべての NAI レルムを削除します。
- **undo nai-realm name** *realm-name* **eap-method** *eap-method-id* コマンドは、同じ名前と EAP 認証方式を使用するすべての NAI レルムを削除します。
- **undo nai-realm name** *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* コマンドは、同じ名前、EAP 認証方式、および認証方式を使用するすべての NAI レルムを削除します。
- **undo nai-realm name** *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* **authentication** *authentication* コマンドは、同じ名前、EAP 認証方式、認証方式、および認証パラメータを使用するすべての NAI レルムを削除します。

Hotspot 2.0 ポリシーには、最大 32 の NAI レルム名を設定できます。

例

Hotspot 2.0 ポリシー1 で NAI レルム test の認証タイプを指定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] nai-realm name test eap-method 2 auth-method 5 authentication 1

4.1.18 network-type

Syntax

network-type *network-type* [**access-internet**]

undo network-type

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

network-type: ネットワークタイプを 0 から 5、14、および 15 の範囲で指定します。

表 4-6 アクセスネットワークタイプ

値	説明
0	プライベートネットワーク
1	ゲストアクセスのプライベートネットワーク
2	有料のパブリックネットワーク
3	無料のパブリックネットワーク
4	パーソナルデバイスネットワーク
5	緊急サービス専用ネットワーク
14	テストまたは実験用
15	ワイルドカード

access-internet: インターネットへのアクセスを有効にします。このキーワードを指定しない場合、インターネットにはアクセスできません。

説明

network-type コマンドはアクセスネットワークタイプを設定します。

undo network-type コマンドはデフォルトに戻します。

アクセスネットワークの種類を設定する前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認してください。

例

アクセスネットワークの種類を 1 に設定し、インターネットへのアクセスを有効にします。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] network-type 1 access-internet

4.1.19 operator-name

Syntax

operator-name *operator-name* **lang-code** *lang-code*

undo operator-name *operator-name* **lang-code** *lang-code*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

operator-name: サービスプロバイダ名を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 言語コードを指定します。デバイスは、ISO 639-1 と ISO 639-2 の両方の規格をサポートしています。

説明

operator-name コマンドはサービスプロバイダ情報を設定します。

undo operator-name コマンドはサービスプロバイダ情報を削除します。

Hotspot 2.0 ポリシーでは、最大 32 個のサービスプロバイダと言語コードの組み合わせを構成できます。

例

サービスプロバイダ example の言語コードを en に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] operator-name example lang-code en

4.1.20 osu-provider

Syntax

osu-provider *osu-provider-number*

undo osu-provider *osu-provider-number*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

osu-provider-number: OSU サーバを 1 から 32 の範囲の番号で指定します。指定された OSU サーバが存在している必要があります。

説明

osu-provider コマンドは OSU サーバを Hotspot 2.0 ポリシーにバインドします。

undo osu-provider コマンドは OSU サーバを Hotspot 2.0 ポリシーからバインド解除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

最大 32 台の OSU サーバを Hotspot 2.0 ポリシーにバインドできます。

OSU サーバを Hotspot 2.0 ポリシーにバインドする前に、次の設定が完了していることを確認してください。

- OSU サーバの名前を設定します。
- OSU サーバの URI を指定します。
- クライアントが OSU サーバと通信するためのプロトコルを指定します。
- OSU サーバのアイコンを指定します。

例

OSU サーバ 1 を Hotspot 2.0 ポリシー1 にバインドします。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] osu-provider 1

関連コマンド

- **friendly-name**
- **icon-file**
- **method**
- **uri**
- **wlan osu-provider**

4.1.21 osu-ssid

Syntax

osu-ssid *ssid-name*

undo osu-ssid

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID 名を指定します。1 から 32 文字の文字列で、大文字と小文字が区別されます。

説明

osu-ssid コマンドはオンラインサインアップサービスの SSID を設定します。

undo osu-ssid コマンドはオンラインサインアップサービス用に設定した SSID を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

オンラインサインアップサービス用に構成された SSID が、オンラインサインアップサービステンプレートの SSID と同じであることを確認します。

例

オンラインサインアップサービスの SSID を osu に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] osu-ssid osu

4.1.22 policy-name

Syntax

policy-name *name*

undo policy-name

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

name: Hotspot 2.0 ポリシー名を 1 から 32 文字の大文字と小文字を区別しない文字列で指定します。

説明

policy-name コマンドは Hotspot 2.0 ポリシーの名前を設定します。

undo policy-name コマンドはデフォルトを復元します。

例

Hotspot 2.0 ポリシー1 の名前を market に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] policy-name market

4.1.23 roam-oi

Syntax

roam-oi *oi* [**in-beacon**]

undo roam-oi *oi*

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

oi: ローミングコンソーシアムを一意に識別できる OI を、6 桁または 10 桁の 16 進数で指定します。

in-beacon: ビーコンに OI を追加します。ベストプラクティスとして、クライアントが OI を取得するには、このキーワードを指定します。

説明

roam-oi コマンドは組織識別子(OI)を設定します。

undo roam-oi コマンドは OI を削除します。

OI を設定する前に、Hotspot 2.0 ポリシーにバインドされているすべてのサービステンプレートが無効になっていることを確認します。Hotspot 2.0 ポリシーでは最大 32 の OI を構成でき、ビーコンには最大 3 つの OI を追加できます。

例

OI を 004096 に設定し、ビーコンに OI を追加します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] roam-oi 004096 in-beacon

4.1.24 uri

Syntax

uri *uri*

undo uri

デフォルト

設定なし

View

OSU server view

定義済みユーザロール

network-admin

パラメータ

uri: OSU サーバの URI を指定します。1 から 255 文字の文字列で、大文字と小文字が区別されます。

説明

uri コマンドは OSU サーバの URI を指定します。

undo uri コマンドは OSU サーバの構成済み URI を削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。クライアントは、構成された URI を使用して OSU サーバにアクセスし、オンラインサインアップを実行します。

OSU サーバがすでに Hotspot 2.0 ポリシーにバインドされている場合、サーバの構成された URI を削除することはできません。

例

OSU サーバ 1 の URI を指定します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1] uri https://osu-server.example.org/

4.1.25 venue group

Syntax

venue group *venue-group-number* **type** *venue-type-number*

undo venue group

デフォルト

設定なし

View

AP view

定義済みユーザロール

network-admin

パラメータ

venue-group-number: 場所グループを番号で指定します。範囲は 1 から 11 です。

表 4-7 場所グループの番号と説明

番号	説明
1	アセンブリ
2	ビジネス
3	教育

番号	説明
4	工場
5	施設
6	商業施設
7	住宅
8	倉庫
9	公共施設
10	車両
11	屋外

venue-type-number: 番号で場所タイプを指定します。値は場所グループ番号によって異なります。詳細については、表 4-8 を参照してください。

表 4-8 場所タイプ番号と説明

場所グループ番号	場所タイプ番号	場所説明
1	0	未指定
1	1	アリーナ
1	2	スタジアム
1	3	旅客ターミナル
1	4	円形劇場
1	5	遊園地
1	6	礼拝所
1	7	会議場
1	8	図書館
1	9	博物館
1	10	レストラン
1	11	劇場
1	12	バー
1	13	喫茶店
1	14	動物園または水族館
1	15	緊急対応センター
2	0	未指定
2	1	医師または歯科医師の診療所
2	2	銀行
2	3	消防署
2	4	警察署

場所グループ番号	場所タイプ番号	場所説明
2	6	郵便局
2	7	専門オフィス
2	8	研究開発施設
2	9	弁護士事務所
3	0	未指定
3	1	小学校
3	2	中学校
3	3	大学
4	0	未指定
4	1	工場
5	0	未指定
5	1	病院
5	2	介護老人保健施設
5	3	アルコール・薬物リハビリテーションセンター
5	4	グループホーム
5	5	刑務所または拘置所
6	0	未指定
6	1	小売店
6	2	食料品市場
6	3	自動車サービスステーション
6	4	ショッピングモール
6	5	ガソリンスタンド
7	0	未指定
7	1	個人住宅
7	2	ホテルまたはモーテル
7	3	宿舎
7	4	下宿
8	0	未指定
9	0	未指定
10	0	未指定
10	1	自動車またはトラック
10	2	飛行機
10	3	バス
10	4	フェリー
10	5	船またはボート

場所グループ番号	場所タイプ番号	場所説明
10	6	電車
10	7	モーターバイク
11	0	未指定
11	1	自治体メッシュネットワーク
11	2	市立公園
11	3	休憩施設
11	4	交通管制施設
11	5	バス停
11	6	売店

説明

venue group コマンドは AP の場所グループ情報を設定します。

undo venue group コマンドはデフォルトに戻します。

例

AP ap3 の場所グループ 1 および場所タイプ 2 を指定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1120

[AC-wlan-ap-ap3] venue group 1 type 2

4.1.26 venue name

Syntax

venue name *venue-name* **lang-code** *lang-code* [**url** *url*]

undo venue name *venue-name* **lang-code** *lang-code* [**url** *url*]

デフォルト

設定なし

View

AP view

定義済みユーザロール

network-admin

パラメータ

venue-name: 場所名を指定します。1 から 252 文字の文字列で、大文字と小文字が区別されます。

lang-code: 場所の言語コードを指定します。デバイスは、ISO 639-1 と ISO 639-2 の両方の標準をサポートしています。

url: AP が属する場所の URL を指定します。1 から 63 文字の文字列で、大文字と小文字は区別されません。URL アドレスには疑問符 (?) を含めることができます。

説明

venue name コマンドは AP の場所名を設定します。

undo venue name コマンドは場所名を削除します。

1 つの場所に複数の言語コードを設定できます。

AP には、最大 32 個の場所名と言語コードの組み合わせを設定できます。

このコマンドで指定する URL は、標準の HTTP または HTTPS プロトコルを介してアクセスでき、http://または https://で始まる必要があります。

例

AP ap3 の場所名を office に、言語コードを en に設定します。

<AC> system-view

[AC] wlan ap ap3 model QX-W1120

[AC-wlan-ap-ap3] venue name office lang-code en

AP ap1 の場所名を v1 に、言語コードを en に、場所 URL を http://www.example.com に設定します。

<AC> system-view

[AC] wlan ap ap1 model QX-W1120

[AC-wlan-ap-ap1] venue name v1 lang-code en url http://www.example.com

4.1.27 wan-metrics

Syntax

wan-metrics { **link-down** | **link-test** | **link-up** } [**asymmetric downlink-speed**

downlink-speed **uplink-speed** *uplink-speed* | **symmetric link-speed**

link-speed]

undo wan-metrics

デフォルト

設定なし

View

Hotspot 2.0 policy view

定義済みユーザロール

network-admin

パラメータ

link-down: WAN のリンクステータスを down に設定します。

link-test: WAN のリンクステータスを testing に設定します。

link-up: WAN のリンクステータスを up に設定します。

asymmetric: 非対称リンクを指定します。

downlink-speed *downlink-speed*: ダウンリンクの速度を 1 から 4194304 Kbps の範囲で指定します。

uplink-speed *uplink-speed*: アップリンクの速度を 1 から 4194304 Kbps の範囲で指定します。

symmetric: 対称リンクを指定します。

link-speed *link-speed*: 対称リンクの速度を 1 から 4194304 Kbps の範囲で指定します。

説明

wan-metrics コマンドは WAN リンクステータスパラメータを設定します。

undo wan-metrics コマンドはデフォルトに戻します。

例

WAN のリンクステータスをアップに、対称リンクレートを 67 Kbps に設定します。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1] wan-metrics link-up symmetric link-speed 67

4.1.28 wlan hotspot-policy

Syntax

wlan hotspot-policy *policy-number*

undo wlan hotspot-policy *policy-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-number: Hotspot 2.0 ポリシーの番号を 1 から 32 の範囲で指定します。

説明

wlan hotspot-policy コマンドは Hotspot 2.0 ポリシーを作成してそのビューを開始するか、既存の Hotspot 2.0 ポリシーのビューを開始します。

undo wlan hotspot-policy コマンドは Hotspot 2.0 ポリシーを削除します。

サービステンプレートにバインドされている Hotspot 2.0 ポリシーは削除できません。

例

Hotspot 2.0 ポリシー1 を作成し、そのビューに入ります。

<AC> system-view

[AC] wlan hotspot-policy 1

[AC-wlan-hs-1]

4.1.29 wlan hotspot osu-icon unload

Syntax

wlan hotspot osu-icon unload

View

System view

定義済みユーザロール

network-admin

説明

wlan hotspot osu-icon unload コマンドはすべての OSU サーバアイコンファイルをアンロードします。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

このコマンドは、OSU サーバアイコンファイルをアンロードするだけで、アイコンファイルは削除されません。

例

すべての OSU サーバアイコンファイルをアンロードします。

<AC> system-view

[AC] wlan hotspot osu-icon unload

関連コマンド

- **icon-file**
- **wlan hotspot osu-icon upload**

4.1.30 wlan hotspot osu-icon upload

Syntax

wlan hotspot osu-icon upload

View

System view

定義済みユーザロール

network-admin

説明

wlan hotspot osu-icon upload コマンドは指定したすべての OSU サーバアイコンファイルをロードします。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

このコマンドを使用して、OSU サーバに指定されたすべてのアイコンファイルを読み込み、アイコンファイルの変更が発生したときに変更を検証します。

例

指定した OSU サーバのアイコンファイルをすべて読み込みます。

<AC> system-view

[AC] wlan hotspot osu-icon upload

関連コマンド

- **icon-file**
- **wlan hotspot osu-icon unload**

4.1.31 wlan osu-provider

Syntax

wlan osu-provider *osu-provider-number*

undo wlan osu-provider *osu-provider-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

osu-provider-number: OSU サーバを 1 から 32 の範囲の番号で指定します。

説明

wlan osu-provider コマンドは OSU サーバを作成してそのビューを開始するか、既存の OSU サーバのビューを開始します。

undo wlan osu-provider コマンドは指定した OSU サーバを削除します。

このコマンドは、Hotspot 2.0 のバージョン 2 でのみ使用できます。

Hotspot 2.0 ポリシーにバインドされている OSU サーバを削除することはできません。

例

OSU サーバ 1 を作成し、そのビューを入力します。

<AC> system-view

[AC] wlan osu-provider 1

[AC-wlan-osu-1]

4.1.32 wlan venue url-unescape-chars

Syntax

wlan venue url-unescape-chars { **composition1** | **composition2** | **custom** *character-string* }

undo wlan venue url-unescape-chars [**custom** *character-string*]

デフォルト

composition1

View

System view

定義済みユーザロール

network-admin

説明

wlan venue url-unescape-chars コマンドは場所 URL のエスケープから特定の特殊文字を除外できます。

undo wlan venue url-unescape-chars コマンドは場所 URL のエスケープから除外された特殊文字を削除できます。

クライアントが特殊文字を構文またはコマンドとして解釈し、意図した意味を変更しないようにするには、これらの文字を安全な形式 (エスケープ文字) に変換する必要があります。

実際には、サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、エラーが発生することがあります。このような場合は、このタスクを実行して、特定の特殊文字をエスケープから除外できます。

場所 URL では、大文字と小文字および数字以外の文字はエスケープする必要がなく、このコマンドを使用して残りの特殊文字を構成できます。

デフォルトでは、デバイスは composition1 の特殊文字をエスケープしません。

サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、例外が発生する場合があります。これに対処するには、これらの特定の文字がエスケープされないように機能を構成します。

例

場所 URL でのエスケープから composition2 の特殊文字を除外します。

<AC> system-view

[AC] wlan venue url-unescape-chars composition2

特殊文字を除く;() が場所 URL でエスケープされないようにします。

<AC> system-view

[AC] wlan venue url-unescape-chars custom ;()

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

13. ユーザアクセスと認証

本マニュアルは以下に示す章で構成されています。

01- WLAN 認証

02-WLAN IP スヌーピング

03-AAA

04-Portal

05-ポートセキュリティ

目次

このセクションのページは **13-x-x** です。

1 章 WLAN 認証 1-1
1.1 WLAN 認証設定コマンド 1-1
1.1.1 client-security accounting-delay time 1-1
1.1.2 client-security accounting-start trigger 1-2
1.1.3 client-security accounting-update trigger 1-3
1.1.4 client-security authentication fail-vlan 1-5
1.1.5 client-security authentication-location 1-6
1.1.6 client-security authentication-mode 1-7
1.1.7 client-security authorization-fail offline 1-8
1.1.8 client-security ignore-authorization 1-9
1.1.9 display dot1x 1-9
1.1.10 display dot1x connection 1-15
1.1.11 display mac-authentication 1-18
1.1.12 display mac-authentication connection 1-24
1.1.13 dot1x authentication-method 1-28
1.1.14 dot1x domain 1-29
1.1.15 dot1x handshake enable 1-30
1.1.16 dot1x handshake secure enable 1-31
1.1.17 dot1x max-user 1-32
1.1.18 dot1x re-authenticate enable 1-33
1.1.19 dot1x retry 1-34
1.1.20 dot1x timer 1-35
1.1.21 fail-permit enable 1-38
1.1.22 fail-permit template 1-38
1.1.23 mac-authentication authentication-method 1-39
1.1.24 mac-authentication domain 1-40
1.1.25 mac-authentication max-user 1-41
1.1.26 mac-authentication timer (system view) 1-42
1.1.27 mac-authentication user-name-format 1-43
1.1.28 reset dot1x statistics 1-45
1.1.29 reset mac-authentication statistics 1-46

1章 WLAN 認証

1.1 WLAN認証設定コマンド

1.1.1 client-security accounting-delay time

Syntax

client-security accounting-delay time *time* [**no-ip-logoff**]

undo client-security accounting-delay time

デフォルト

課金開始要求は、無線クライアントの IP アドレスが学習されるまで課金サーバに対して開始されない。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

time time:課金遅延時間。1~600 の範囲で秒単位で指定できます。

no-ip-logoff:デバイスが指定された遅延時間内にワイヤレスクライアントの IP アドレスを取得しない場合は、クライアントをオフラインにします。このパラメータを指定しない場合、デバイスは、指定された課金遅延時間に達すると、課金開始要求メッセージを送信します。

説明

client-security accounting-delay time コマンドを使用して、課金遅延機能を有効にします。

undo client-security accounting-delay time コマンドを使用して、デフォルトに戻します。

指定された課金遅延時間内に装置が指定されたタイプのクライアントの IP アドレスを学習しない場合、対応する課金遅延動作が実行される。課金開始をトリガするワイヤレスクライアント IP アドレスタイプは、**client-security accounting-start trigger** コマンドの設定によって決まります。クライアント IP アドレスタイプが none の場合、課金遅延機能は有効になりません。

課金遅延時間は、機器が IP アドレスを取得する時間の長さに応じて設定することが推奨され、機器が IP アドレスを取得する時間が長くなるネットワーク環境が悪い場合には、この値を適宜大きくすることができる。

無線サービステンプレートを起動した後に本機能を設定すると、設定は新たにオンラインになったクライアントに対してのみ有効となり、すでにオンラインになっているクライアントに対しては無効となる。

例

#サービステンプレート service1 の下で、請求遅延時間を 15 秒に設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] client-security accounting-delay time 15 no-ip-logoff

関連コマンド

- **client-security accounting-start trigger**

1.1.2 client-security accounting-start trigger

Syntax

client-security accounting-start trigger { **ipv4** | **ipv4-ipv6** | **ipv6** | **none** }

undo client-security accounting-start trigger

デフォルト

トリガ課金が開始される無線クライアントの IP アドレスタイプは IPv4 です。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

IPv4:無線クライアントの IP アドレスタイプが IPv4 であることを示します。

ipv4-ipv6:ワイヤレスクライアントの IP アドレスタイプが IPv4 または IPv6 であることを示します。

ipv6:無線クライアントの IP アドレスタイプが IPv6 であることを示します。

none:デバイスが無線クライアント認証に成功すると課金開始要求メッセージを送信することを示す。

本装置では ipv4-ipv6、ipv6 をサポートしていません。

説明

client-security accounting-start trigger コマンドを使用して、課金開始をトリガするワイヤレスクライアントの IP アドレスタイプを設定します。

undo client-security accounting-start trigger コマンドを使用して、デフォルトに戻します。

無線クライアントが 802.1X 認証または MAC アドレス認証方式によってオンラインになると、設備は課金開始をトリガする無線クライアントの IP アドレスのタイプによって課金サーバに課金開始要求メッセージを送信するかどうかを決定し、課金サーバが課金開始応答メッセージを返した後にクライアントへの課金を開始する。

ワイヤレスクライアントの IP アドレスタイプを設定すると、設定が有効になるまで、そのタイプのクライアントアドレス学習機能を有効にする必要があります。有効にしないと、課金が開始されません。クライアントアドレス学習機能の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*2 章 WLAN IP スヌーピング*“を参照してください。

このコマンドで設定するワイヤレスクライアントの IP アドレスタイプは、課金サーバのプロトコル要件を満たす必要があります。

無線サービステンプレートが起動した後、この機能を再配置すると、新しい配置は新しくオンラインになったクライアントにだけ有効で、すでにオンラインになったクライアントには無効です。

例

#サービステンプレート service1 で、課金開始をトリガするワイヤレスクライアントの IP アドレスタイプを IPv4 に設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] client-security accounting-start trigger ipv4

関連コマンド

- **client ipv4-snooping arp-learning enable (ユーザアクセスと認証-WLAN IP スヌーピング)**
- **client ipv4-snooping dhcp-learning enable (ユーザアクセスと認証-WLAN IP スヌーピング)**
- **client-security accounting-delay**
- **client-security accounting-update trigger**

1.1.3 client-security accounting-update trigger

Syntax

client-security accounting-update trigger { **ipv4** | **ipv4-ipv6** | **ipv6** }

undo client-security accounting-update trigger

デフォルト

課金更新要求メッセージは、課金サーバによって送信される時間間隔またはデバイスによって構成されるリアルタイム課金に基づいて周期的に送信される。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

IPv4:無線クライアントの IP アドレスタイプが IPv4 であり、デバイスがクライアントの IPv4 アドレスの変更を学習した場合にのみ課金更新要求メッセージを送信することを示します。

ipv4-ipv6:無線クライアント IP アドレスタイプが IPv4 または IPv6 であることを示し、デバイスはクライアント IP アドレスの変化を学習するたびに課金更新要求メッセージを送信する。

ipv6:無線クライアントの IP アドレスタイプが IPv6 であり、デバイスがクライアントの IPv6 アドレスの変更を学習した場合にのみ課金更新要求メッセージを送信することを示す。

本装置では ipv4-ipv6、ipv6 をサポートしていません。

説明

client-security accounting-update trigger コマンドを使用して、課金更新をトリガするワイヤレスクライアントの IP アドレスタイプを設定します。

undo client-security accounting-update trigger コマンドを使用して、デフォルトに戻します。

課金更新をトリガするワイヤレスクライアント IP アドレスタイプの設定は、課金開始をトリガするワイヤレスクライアント IP アドレスタイプの設定が有効になっている場合にのみ有効になります。

設定が完了すると、設定と定期的に課金更新メッセージを送信する機能が同時に有効になります。

課金更新をトリガするように構成された無線クライアント IP アドレスタイプが IPv4 であり、課金更新メッセージを周期的に送信するように構成されたリアルタイム課金間隔が 12 分(**timer realtime-accounting** コマンドの設定)であると仮定すると、デバイスは、12 分毎に課金更新要求を開始し、オンラインクライアント IPv4 アドレスが変化すると、課金更新要求メッセージを直ちに送信する。

無線サービステンプレートを起動した後に本機能を設定すると、設定は新たにオンラインになったクライアントに対してのみ有効となり、すでにオンラインになっているクライアントに対しては無効となる。

例

#サービステンプレートで、課金更新をトリガするクライアント IP アドレスタイプを IPv4 に設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] client-security accounting-update trigger ipv4

関連コマンド

- **client-security accounting-start trigger**
- **timer realtime-accounting (ユーザアクセスと認証-AAA)**

1.1.4 client-security authentication fail-vlan

Syntax

client-security authentication fail-vlan *vlan-id*

undo client-security authentication fail-vlan

デフォルト

認証失敗 VLAN が設定されていません。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

vlan-id:認証に失敗した VLAN の VLAN ID。範囲は 1~4094 です。

説明

client-security authentication fail-vlan コマンドを使用して、サービステンプレートの下の認証失敗 VLAN を設定します。

undo client-security authentication fail-vlan コマンドを使用して、デフォルトに戻します。

ここでの認証失敗とは、認証サーバが何らかの理由でユーザの認証を明示的に拒否することであり、たとえばユーザのパスワードが間違っていたり、認証がタイムアウトしたり、ネットワークに接続していなかったりすることによるものではない。

設定認証に失敗した VLAN は、すでに存在する VLAN である必要があります。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

例

#サービステンプレート 1 の下で認証失敗 VLAN を VLAN 10 に設定します。

<Sysname> sysname-view

[Sysname] wlan service-template 1

[Sysname-wlan-st-1] client-security authentication fail-vlan 10

1.1.5 client-security authentication-location

Syntax

client-security authentication-location { **ac** | **ap** }

undo client-security authentication-location

デフォルト

WLAN ユーザアクセス認証場所は AC にあります。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ac:WLAN ユーザが AC 上の認証ロケーションにアクセスしていることを示します。

ap:AP 上の WLAN ユーザアクセス認証場所を設定します。

説明

WLAN ユーザアクセス認証の場所を設定するには、**client-security authentication-location** コマンドを使用します。

undo client-security authentication-location コマンドを使用して、デフォルトに戻します。

クライアントのデータグラム転送先が AC の場合、設定されたユーザアクセス認証先を AP にすることはできません。AP にすると、ユーザ認証が失敗します。クライアントデータメッセージの転送先コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*6 WLAN アクセス*”の”*1 章 WLAN アクセス*”を参照してください。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

例

#AC のクライアントのためのユーザ認証場所を設定します。

<Sysname> system-view

[Sysname] wlan service-template s1

[Sysname-wlan-st-s1] client-security authentication-location ac

関連コマンド

- **client forwarding-location (WLAN アクセス-WLAN アクセス)**

1.1.6 client-security authentication-mode

Syntax

client-security authentication-mode { **dot1x** | **mac** | **mac-and-dot1x** }

undo client-security authentication-mode

デフォルト

ユーザへのアクセス認証である Bypass 認証は行わない。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot1x:802.1X 認証のみを行うことを示す。

mac:MAC アドレス認証のみを行うことを示す。

mac-and-dot1x:MAC アドレス認証と 802.1X 認証の両方を行うことを示す。MAC アドレス認証を先に行い、失敗した場合は認証を行わない。認証に成功すると、802.1X 認証が追加されます。

説明

client-security authentication-mode コマンドを使用して、ワイヤレスユーザアクセス認証モードを設定します。

undo client-security authentication-mode コマンドを使用して、デフォルトに戻します。

以上の各モードでは、無線サービステンプレートごとに複数の認証済みユーザへのアクセスが許可される。802.1X ユーザの数は **dot1x max-user** コマンドによって設定され、MAC アドレス認証ユーザの数は **mac-authentication max-user** コマンドによって設定されます。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

例

#サービステンプレート service1 で MAC アドレス認証モードのワイヤレスユーザアクセス認証モードを設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] client-security authentication-mode mac

1.1.7 client-security authorization-fail offline

Syntax

client-security authorization-fail offline

undo client-security authorization-fail offline

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

client-security authorization-fail offline コマンドを使用して、認証に失敗したユーザのオフライン機能を有効にします。

undo client-security authorization-fail offline コマンドを使用して、認証が失敗した後のユーザのオフライン機能を無効にします。

許可失敗後のユーザのオフライン機能が有効になっている場合、許可 ACL、User Profile が存在しない場合、許可 ACL、User Profile が削除された場合、または ACL、User Profile が失敗した場合、ユーザは強制的にオフラインになります。

許可失敗後のサブスクライバのドロップダウン機能が有効になっていない場合、ドロップされた許可 ACL、User Profile が存在しない場合、許可 ACL、User Profile が削除される場合、または ACL、User Profile のドロップダウンが失敗した場合、サブスクライバはオンラインのままになり、許可 ACL、User Profile は有効にならず、デバイスは Log 情報を出力します。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

例

#サービステンプレート service1 で認証が失敗しましたユーザのオフライン機能を有効にします。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] client-security authorization-fail offline

1.1.8 client-security ignore-authorization

Syntax

client-security ignore-authorization

undo client-security ignore-authorization

デフォルト

RADIUS サーバまたはデバイスからローカルに送信された認証情報を適用します。

View

Service template view

定義済みユーザロール

network-admin

説明

client-security ignore-authorization コマンドは、RADIUS サーバまたはデバイスからローカルに送信された認証情報を無視するように設定するために使用します。

undo client-security ignore-authorization コマンドを使用して、デフォルトに戻します。

ユーザが RADIUS 認証またはローカル認証に合格すると、RADIUS サーバまたはデバイスは、ユーザアカウントに設定された関連する属性に基づいて、ダイナミック VLAN ダウンなどの認証を行います。このような動的に送信される許可属性を受け入れたくない場合は、このコマンドを設定して無視できます。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

例

#サービステンプレート service1 で、RADIUS サーバまたはデバイスからローカルに送信された認証情報を無視するように設定します。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] client-security ignore-authorization
```

1.1.9 display dot1x

Syntax

display dot1x [**sessions** | **statistics**] [**ap** *ap-name* [**radio** *radio-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

sessions:802.1X のセッション接続情報を表示します。

statistics:802.1X に関する統計情報を表示します。

ap *ap-name*:指定した AP のすべての 802.1X の詳細を表示します。ap-name は AP の名前です。1~64 文字の文字列で、英数字、アンダースコア、[」 、 「]、 「/」 、 「-」 を使用でき、大文字と小文字が区別されます。

radio *radio-id*:Radio を指定したすべての 802.1X の詳細を表示します。radio-id は Radio 番号を表し、デバイスモデルに関連する値の範囲を取ります。このパラメータを指定しないと、指定した AP のすべての Radio の 802.1X の詳細が表示されます。

説明

display dot1x コマンドを使用して、802.1X に関する情報を表示します。

sessions または statistics パラメータを指定しない場合は、セッション接続情報、関連する統計情報、構成情報など、802.1X に関するすべての情報が表示されます。

ap パラメータを指定しない場合は、すべての 802.1X 情報が表示されます。

例

#802.1X のすべての情報を表示します。

<Sysname> display dot1x

```
Global 802.1X parameters:
  802.1X authentication                   : Enabled
  M-LAG member configuration conflict       : Unknown
  EAP authentication                      : Enabled
  Max-tx period                           : 30 s
  Handshake period                        : 15 s
  Offline detect period                   : 300 s
  Quiet timer                             : Disabled
       Quiet period                       : 60 s
  Supp timeout                            : 30 s
  Server timeout                          : 100 s
  Reauth period                           : 3600 s
  Max auth requests                       : 2
  SmartOn supp timeout                    : 30 s
  SmartOn retry counts                    : 3
```

```
  User aging period for Auth-Fail VLAN      : 1000 s
  User aging period for critical VLAN       : 1000 s
  User aging period for guest VLAN          : 1000 s
  EAD assistant function                   : Disabled
     URL                                  : http://www.dwsoft.com
     Free IP                               : 6.6.6.0       255.255.255.0
     EAD timeout                           : 30 min
  Domain delimiter                         : @
  Max EAP-TLS fragment (to-server)          : 400 bytes
Online 802.1X wired users                  : 1
Online 802.1X wireless users               : 1

AP name: AP1  Radio ID: 1  SSID: wlan_dot1x_ssid
  BSSID                   : 1111-1111-1111
  802.1X authentication     : Enabled
  Handshake                : Enabled
  Handshake security        : Disabled
  Periodic reauth          : Disabled
  Mandatory auth domain     : Not configured
  Max online users          : 256

  EAPOL packets: Tx 3, Rx 3
  Sent EAP Request/Identity packets : 1
      EAP Request/Challenge packets: 1
      EAP Success packets: 1
      EAP Failure packets: 0
  Received EAPOL Start packets : 1
      EAPOL LogOff packets: 1
      EAP Response/Identity packets : 1
      EAP Response/Challenge packets: 1
      Error packets: 0
  Online 802.1X users: 1
        MAC address       Auth state
        0001-0000-0002     Authenticated
```

表 1-1 display dot1x コマンドの表示情報の説明

フィールド	説明
Global 802.1X parameters	グローバル802.1Xパラメータ構成情報
802.1X authentication	グローバル802.1Xの状態

フィールド	説明
DR member configuration conflict	(未サポート) 2台のDRデバイス構成チェック結果 ● **Conflicted**:両方のDRデバイスで構成が一致していない ● **Not conflicted**:2つのDRデバイスで構成された一致 ● **Unknown**:両方のDRデバイスで構成が一致するかどうかを検出できません
CHAP authentication	CHAP認証を使用したEAP-Endモードの有効化
EAP authentication	EAPリレー方式を有効にし、すべてのEAP認証方式をサポートする
PAP authentication	EAP-Terminationモードを有効にし、PAP認証方式を採用
Max-tx period	ユーザ名リクエストタイムアウトタイマの値
Handshake period	ハンドシェイクタイマの値
Offline detect period	オフライン検出タイマの値
Quiet timer	サイレントタイマの状態
Quiet period	サイレントタイマの値
Supp timeout	クライアント認証タイムアウトタイマの値
Servertimeout	認証サーバのタイムアウトタイマの値
Reauth period	再認証タイマの値
Max auth requests	デバイスがアクセスユーザに認証要求メッセージを送信する最大回数
User aging period for Auth-Fail VLAN	Auth-Fail VLANでのユーザの経過時間
User aging period for critical VLAN	Critical VLANでのユーザの経過時間
User aging period for guest VLAN	Guest VLANでのユーザの経過時間
EAD assistant function	EAD Quick Deploymentのアクセシビリティが有効になっている状態
URL	ユーザHTTPアクセスのリダイレクトURL
Free IP	ユーザが認証される前にアクセスできるネットワークセグメント
EAD timeout	EADエージングタイマのタイムアウト
Domain delimiter	ドメイン名デリミタ
Max EAP-TLS fragment (to-server)	認証サーバに送信する認証メッセージに含まれるEAP-TLSフラグメントのメッセージの最大長 EAP-TLSシャードメッセージの最大長が設定されていない場合は、N/Aと表示されます。
Online 802.1X wired users	オンラインの802.1X有線ユーザと、認証を開始している802.1X有線ユーザの合計数
Online 802.1X wireless users	オンラインの802.1Xワイヤレスユーザと、認証を開始している802.1Xワイヤレスユーザの合計数
GigabitEthernet1/0/1 is link-up	ポートGigabitEthernet1/0/1のリンクステータス
802.1X authentication	ポートでの802.1Xの状態
Handshake	オンラインユーザハンドシェイク機能の状態
Handshake reply	オンラインユーザハンドシェイク応答機能の状態
Handshake security	セキュア・ハンドシェイク機能の状態

フィールド	説明
Offline detection	802.1X認証オフラインテストの状態 ● **Enabled**:有効 ● **Disabled**:無効 ● **Enabled (NOT effective)**:有効になっていますが、動作していません。ドロップ検出機能を有効にした場合、ポートアクセス制御方式をPort-basedに変更した場合に表示される.
Unicast trigger	802.1Xユニキャストトリガ機能の状態
Periodic reauth	周期的再認証機能の状態
Port role	このポートは認証側として機能し、現在は認証側としてのみサポートされています。
Authorization mode	ポートの承認ステータス ● **Force-Authorized**:強制承認ステータス ● **Auto Auto Auto**:状態の自動認識 ● **Force-Unauthorized**:不正な状態の強制
Port access control	ポートアクセス制御方式 ● **MAC-based**:MACアドレスに基づいてユーザを認証する ● **Port-based**:ポートに基づいたユーザ認証
Multicast trigger	802.1Xマルチキャストトリガー機能の状態
Mandatory auth domain	ポート上のアクセスユーザが使用する必須認証ドメイン
Guest VLAN	ポートが設定されている場合はGuest VLAN、この機能が設定されていない場合はNot configured
Auth-fail VLAN	ポートが設定されている場合はAuth-Fail VLAN、この機能が設定されていない場合はNot configured
Critical VLAN	ポートが設定されている場合はCritical VLAN、この機能が設定されていない場合はNot configured
Critical voice VLAN	(未サポート)ポート設定802.1X認証Critical Voice VLAN機能は、次の値で有効になっています。 ● **Enabled**:有効 ● **Disabled**:無効
Add Guest VLAN delay	ポート遅延加入Guest VLAN機能の状態およびトリガ原因: ● **EAPOL**:802.1Xプロトコルメッセージトリガーポート遅延加入802.1X Guest VLAN ● **NewMac**:送信元MACアドレスが不明なメッセージがトリガされ、ポートが802.1に加入するまで遅延しますX Guest VLAN ● **ALL**:802.1Xプロトコルメッセージまたは送信元MACアドレス不明のメッセージポート遅延加入802.1X Guest VLAN ● **Disabled**:無効
Re-auth server-unreachable	再認証時にサーバが802.1Xオンラインユーザに到達できないアクション

フィールド	説明
Max online users	このポートの最大アクセスユーザ数
User IP freezing	802.1XユーザIPアドレス凍結機能の状態 ● **Enabled**:有効 ● **Disabled**:無効
Reauth period	ポートの802.1X定期再認証タイマの値
Send Packets Without Tag	ポートはVLAN Tagの状態を運ばない802.1Xプロトコルメッセージを送信します。 ● **Enabled**:有効 ● **Disabled**:無効
Max Attempts Fail Number	MACアドレス認証に成功したユーザによる802.1X認証の最大試行回数
User aging	非認証成功マイクロセグメンテーション、VLANの802.1Xユーザエージング機能状態 ● **Enabled**:有効 ● **Disabled**:無効
Server-recovery online-user-sync	RADIUSサーバが到達不能状態から到達可能状態に戻ると、デバイスは802.1Xオンラインユーザ情報をRADIUSサーバ機能が有効になっている状態に同期します。 ● **Enabled**:有効 ● **Disabled**:無効
Auth-Fail EAPOL	802.1XユーザがAuth-Fail VLANに参加すると、デバイス側はクライアントにEAP-Successメッセージ機能が有効になっていることを通知します。 ● **Enabled**:有効 ● **Disabled**:無効
Critical EAPOL	802.1XユーザがCritical VLANに参加すると、デバイス側はクライアントにEAP-Successメッセージ機能が有効になっていることを通知します。 ● **Enabled**:有効 ● **Disabled**:無効
Discard duplicate EAPOL-Start	802.1Xユーザ認証プロセス中にデバイスが重複するEAPOL-Startメッセージを廃棄するかどうか。 ● **Yes**:破棄 ● **No**:破棄しません
EAPOL packets	EAPOLメッセージ数。Txは送信されたメッセージ数を表す.;Rxは受信メッセージ数を表す.
Sent EAP Request/Identity packets	送信されたEAP Request/Identityメッセージの数
EAP Request/Challenge packets	送信されたEAP Request/Challengeメッセージの数

フィールド	説明
EAP Success packets	送信されたEAP Successメッセージの数
EAP Fail packets	送信されたEAP Failureメッセージの数
Received EAPOL Start packets	受信したEAPOL Startメッセージの数
EAPOL LogOff packets	受信したEAPOL LogOffメッセージの数
EAP Response/Identity packets	受信したEAP Response/Identityメッセージの数
EAP Response/Challenge packets	受信したEAP Response/Challengeメッセージの数
Error packets	受信したエラーメッセージの数
Online 802.1X users	ポート上のオンライン802.1Xユーザと、認証を開始している802.1Xユーザの合計数
MAC address	802.1XユーザのMACアドレス
Auth state	802.1Xユーザの認証ステータス
AP name	AP名
Radio ID	Radio番号
SSID	サービスセット識別子
BSSID	基本サービスセット識別子

1.1.10 display dot1x connection

Syntax

display dot1x connection [**ap** *ap-name* [**radio** *radio-id*] | **slot** *slot-number* |**user-mac** *mac-address* | **user-name** *name-string*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*:指定した AP にアクセスするすべての 802.1X オンラインユーザの情報を表示します。ap-name は AP の名前です。1~64 文字の文字列で、英数字、「 _ 」、「 [」、「] 」、 「 / 」 、 「 - 」 を使用でき、大文字と小文字が区別されます。このパラメータを指定しない場合、デバイス上のすべての 802.1X オンラインユーザの情報が表示されます。

radio *radio-id*:指定された Radio にアクセスする 802.1X オンラインユーザの情報を表示します。radio-id は Radio 番号を表し、デバイスモデルに関連する値の範囲を取ります。このパラメータを指定しないと、AP の下のすべての Radio にアクセスする 802.1X オンラインユーザの情報が表示されます。

slot *slot-number:*クラウドクラスタメンバーデバイスをそのメンバーID で指定します。メンバーデバイスを指定しない場合、このコマンドはすべてのメンバーデバイスのオンライン 802.1X オンラインユーザに関する情報を表示します。

user-mac *mac-address*:指定した MAC アドレスの 802.1X オンラインユーザ情報を表示します。ここで、mac-address はユーザの MAC アドレスで、H-H-H の形式です。このパラメータを指定しない場合、デバイス上のすべての 802.1X オンラインユーザの情報が表示されます。

user-name *name-string*:指定したユーザ名の 802.1X オンラインユーザ情報を表示します。ここで、name-string はユーザ名を表します。は 1~253 文字の文字列で、大文字と小文字が区別されます。このパラメータを指定しない場合、デバイス上のすべての 802.1X オンラインユーザの情報が表示されます。

説明

display dot1x connection コマンドを使用して、現在の 802.1X オンラインユーザの詳細を表示します。

例

#802.1X のすべてのオンラインユーザ情報を表示します。

<Sysname> display dot1x connection

```
Total connections: 1

Slot ID: 1
User MAC address             : 0015-e9a6-7cfe
AP name                     : ap1
Radio ID                    : 1
SSID                        : wlan_dot1x_ssid
BSSID                       : 0015-e9a6-7cf0
User name                   : ias
Anonymous username           : test
Authentication domain        : 1
IPv4 address                : 192.168.1.1
IPv6 address                : 2000:0:0:0:1:2345:6789:abcd
Authentication method        : CHAP
Initial VLAN                : 1
Authorization VLAN           : N/A
Authorization ACL number      : 3001
Authorization user profile    : N/A
Authorization CAR            : N/A
Authorization URL            :
Authorization IPv6 URL        : N/A
Termination action           : Default
Session timeout last from    : 2023/05/30 17:32:42
```

```
Session timeout period       : 86400 s
Online from                 : 2023/05/30 11:20:41
Online duration              : 6h 18m 39s
```

表 1-2 display dot1x connection コマンドの表示情報の説明

フィールド	説明
Total connections	オンライン802.1 Xユーザの数
User MAC address	ユーザのMACアドレス
Access interface	ユーザがデバイスにアクセスするためのインタフェース
AP name	ユーザが関連付けられているAPの名前
Radio ID	ユーザが関連付けられている無線のID
SSID	ユーザが関連付けられているSSID
BSSID	ユーザが関連付けられているBSSのID
User access state	ユーザのアクセス状態 ● **Successful**—ユーザは802.1 X認証に合格し、オンラインになります。 ● **Open**—ユーザは存在しないユーザ名または誤ったパスワードを使用して、オープン認証モードでオンラインになります。
Authentication domain	802.1 X認証に使用されるISPドメイン
IPv4 address	ユーザのIPv 4アドレス デバイスがユーザのIPv 4アドレスを取得しない場合、このフィールドは使用できません。
IPv6 address	ユーザのIPv 6アドレス デバイスがユーザのIPv 6アドレスを取得しない場合、このフィールドは使用できません。
Authentication method	EAPメッセージ処理方式: ● **CHAP**— EAP終了を実行し、CHAPを使用してRADIUSサーバと通信します。 ● **EAP**— EAPパケットをリレーし、任意のEAP認証方式をサポートしてRADIUSサーバと通信します。 ● **PAP**— EAP終了を実行し、PAPを使用してRADIUSサーバと通信します。
Initial VLAN	802.1 X認証前にユーザが所属していたVLAN
Authorization untagged VLAN	ユーザに許可されたタグなしVLAN。
Authorization tagged VLAN list	ユーザに許可されたタグ付きVLAN。
Authorization ACL number/name	ユーザに許可されたACLの番号または名前 許可ACLが割り当てられていない場合、このフィールドにはN/Aと表示されます。 ACL許可が失敗した場合、このフィールドにはACLの横に (Not effective) と表示されます。
Authorization user profile	ユーザに許可されたユーザプロファイル

フィールド	説明
Authorization CAR	サーバによって割り当てられた認可CAR属性 ● **Average input rate**:着信トラフィックの平均レート（bps単位）。 ● **Peak input rate**:着信トラフィックのピークレート（bps単位）。 ● **Average output rate**:発信トラフィックの平均レート（bps単位）。 ● **Peak output rate**:発信トラフィックのピークレート（bps単位）。 デバイスがCAR属性のユーザへの割り当てに失敗した場合、[Authorization CAR] フィールドに（NOT effective）と表示されます。 サーバがピークレートを割り当てない場合、デフォルトのピークレートは割り当てられた平均レートと同じになります。現在のソフトウェアバージョンでは、デバイスはサーバからのピークレートの排他的割り当てをサポートしていません。 認可CAR属性が割り当てられていない場合、このフィールドにはN/Aと表示されます。
Authorization URL	ユーザに許可されたリダイレクトURL
Authorization IPv6 URL	ユーザに許可されたリダイレクトIPv 6 URL
Termination action	ユーザセッションを終了するためにサーバによって割り当てられたアクション属性: ● **Default**:サーバによって割り当てられたセッションタイムアウトタイマーが期限切れになると、オンライン認証された802.1 Xユーザをログオフします。802.1 X定期再認証が有効で、定期再認証タイマがサーバによって割り当てられたセッションタイムアウトタイマより短い場合、この属性は有効になりません。 ● **Radius-request**:802.1 X定期再認証機能が有効かどうかに関係なく、サーバによって割り当てられたセッションタイムアウトタイマーが期限切れになったときにオンラインユーザを再認証します。 デバイスがローカル認証を実行する場合、このフィールドにはDefaultと表示されます。
Session timeout period	サーバによって割り当てられたセッションタイムアウトタイマ
Online from	802.1 Xユーザがオンラインになった時刻
Online duration	802.1 Xユーザのオンライン期間

1.1.11 display mac-authentication

Syntax

display mac-authentication [**ap** *ap-name* [**radio** *radio-id*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*:指定した AP のすべての MAC アドレス認証の詳細を表示します。ap-name は AP の名前です。1~64 文字の文字列で、英数字、「 _ 」、「 [」、 「] 」、 「 / 」 、「 - 」 を使用でき、大文字と小文字が区別されます。

radio *radio-id*:Radio を指定したすべての MAC アドレス認証の詳細を表示します。radio-id は Radio 番号を表し、デバイスモデルに関連する値の範囲を取ります。このパラメータを指定しない場合、指定した AP のすべての Radio の MAC アドレス認証の詳細が表示されます。

説明

display mac-authentication コマンドは、MAC アドレス認証に関する情報を表示します。

パラメータを指定しない場合は、すべてのオンライン MAC アドレス認証の詳細が表示されます。これには、グローバルおよびポートの構成情報、認証メッセージ統計、認証ユーザ情報が含まれます。

例

#MAC アドレスの認証情報を表示します。

<Sysname> display mac-authentication

```
Global MAC authentication parameters:
  MAC authentication                     : Enabled
  Authentication method                  : PAP
  M-LAG member configuration conflict      : Unknown
  Username format                        : MAC address in lowercase(xx-xx-xx-
xx-xx-xx)
         Username                      : mac
         Password                      : Not configured
  MAC range accounts                     : 0
        MAC address        Mask              Username
  Offline detect period                  : 300 s
  Quiet period                           : 60 s
  Server timeout                         : 100 s
  Reauth period                          : 3600 s
  User aging period for critical VLAN      : 1000 s
  User aging period for guest VLAN         : 1000 s
```

```
  Authentication domain                        : Not configured, use default
domain
  HTTP proxy port list                    : Not configured
  HTTPS proxy port list                   : Not configured
  Online MAC-auth wired users               : 0
  Online MAC-auth wireless users            : 1

 Silent MAC users:
        MAC address      VLAN ID  From port            Port index

 AP name: AP1  Radio ID: 1  SSID: wlan_maca_ssid
  BSSID                   : 1111-1111-1111
 MAC authentication         : Enabled
  Authentication domain     : Not configured
  Max online users          : 256
  Authentication attempts   : successful 1, failed 0
  Current online users      : 2
        MAC address      Auth state
        0001-0000-0002    Authenticated
        0001-0000-0003    Unauthenticated
```

表 1-3 display mac-authentication コマンドの表示情報の説明

フィールド	説明
Global MAC authentication parameters	グローバルMACアドレス認証パラメータ
MAC authentication	MACアドレス認証の状態 この機能の有効性はデバイスのモデルに依存します。デバイスの実際の状態に基づいてください。
DR member configuration conflict	(未サポート) 2台のDRデバイス構成チェック結果 • Conflicted:両方の DR デバイスで構成が一致していない • Not conflicted:2 つの DR デバイスの構成が一致する • Unknown:両方の DR デバイスで構成が一致するかどうかを検出できません
Authentication method	MACアドレス認証に用いる認証方法 • CHAP CHAP:CHAP 認証方式を使用します。 • PAP:PAP 認証方式の使用

フィールド	説明
Username format	MACアドレス認証に使用するアカウント番号の形式 • MAC アドレス番号を使用する場合は、特定のユーザ名の形式、ハイフンの有無、アルファベットの大文字と小文字が表示されます。たとえば、この例の「MAC address in lowercase (xx-xx-xx-xx-xx-xx)」は、ユーザ名の形式が 6 段階の MAC アドレスで、アルファベットは小文字です。 • 固定アカウント名の場合は、「Fixed account」と表示されます。
Username	ユーザ名 • MAC アドレスアカウントを使用している場合、この値は「mac」と表示されますが、実際の意味はなく、ユーザ名とパスワードに MAC アドレスを使用していることを示します。 • 固定ユーザ名アカウントの場合、この値は設定されたユーザ名(デフォルトは mac です。)です。
Password	ユーザ名のパスワード • MAC アドレスアカウントを使用すると、値は「Not configured」と表示されます。 • 固定ユーザ名アカウントの場合、設定された値は******と表示されます。
Offline detect period	オフライン検出タイマの値
Quiet period	サイレントタイマの値
Server timeout	サーバ接続タイムアウトタイマの値
Reauth period	再認証タイマの値
User aging period for critical VLAN	Critical VLANでのユーザの経過時間
User aging period for guest VLAN	Guest VLANでのユーザの経過時間
Authentication domain	System viewで指定されたMACアドレスは、ユーザが使用する認証ドメインを認証します。認証ドメインが指定されていない場合は、Not configured, use default domainと表示されます。
Online MAC-auth wired users	MACアドレス認証を開始しているオンライン有線ユーザと有線ユーザの合計数
Online MAC-auth wireless users	オンライン無線ユーザとMACアドレス認証を開始している無線ユーザの合計数

フィールド	説明
Silent MAC users	サイレントユーザ情報(デバイスによって追加されたサイレントユーザおよびサーバ許可が含まれていますブラックホールMACのサイレントユーザ)
MAC address	サイレントユーザのMACアドレス
VLAN ID	サイレントユーザのVLAN
From port	サイレント・ユーザ・アクセスのポート名
Port index	サイレント・ユーザ・アクセスのポート・インデックス番号
GigabitEthernet1/0/1 is link-up	ポートGigabitEthernet1/0/1のリンクステータス
MAC authentication	現在のポートのMACアドレス認証の状態 • Enabled:有効 • Enabled (but NOT effective):有効ですが、動作していません。未有効理由デバイス上の ACL リソースがすべて使用されています • Disabled:無効
Carry User-IP	MACアドレス認証要求携帯ユーザIPアドレス状態
Authentication domain	ポートで指定されたMACアドレス認証ユーザが使用する認証ドメイン
Auth-delay timer	MACアドレス認証遅延機能の状態
Auth-delay period	構成済みの認証遅延時間
Periodic reauth	ポートでのMACアドレス再認証の状態
Reauth period	ポートで設定されたMACアドレス再認証間隔
Re-auth server-unreachable	再認証時にサーバがMACアドレス認証のためのオンラインユーザに到達できない動作 • Logoff:再認証サーバにアクセスできないため、MAC アドレス認証をオンラインユーザに強制的にオフラインにする • Online:再認証サーバにアクセスできないため、MAC アドレス認証をオンラインユーザに維持
Guest VLAN	ポートが設定されている場合はGuest VLAN、設定されていない場合はNot configured
Guest VLAN reauthentication	Guest VLANでのユーザ再認証機能の状態 • Enabled:有効 • Disabled:無効

フィールド	説明
Guest VLAN auth-period	Guest VLANに入ってから再認証が開始されるまでの時間間隔
Critical VLAN	ポートが設定されている場合はCritical VLAN、設定されていない場合はNot configured
Host mode	同じMACアドレスユーザの動作モード • マルチ VLAN モードが設定されている場合は、Multiple VLAN と表示されます。 • シングル VLAN モードが設定されている場合は、Single VLAN と表示されます。
Offline detection	MACアドレス認証ユーザのオフライン検出の状態 • Enabled:有効 • Disabled:無効
Authentication order	MACアドレス認証と802.1 X認証の並列処理 • Default:有効 • Parallel:無効
User aging	非認証成功中のMACアドレス認証ユーザエージング機能の状態 • Enabled:有効 • Disabled:無効
Server-recovery online-user-sync	RADIUSサーバが到達不能状態から到達可能状態に戻ると、デバイスはMACアドレス認証のためのオンラインユーザ情報をRADIUSサーバ機能が有効になっている状態に同期します。 • Enabled:有効 • Disabled:無効
Auto-tag feature	ポートでのMACアドレス認証VLAN自動タグ機能の承認 • Enabled:有効 • Disabled:無効
VLAN tag configuration ignoring	ポートのMACアドレス認証VLAN自動タグ無視静的VLAN設定機能 • Enabled:有効 • Disabled:無効
Max online users	このポートの最大アクセスユーザ数

フィールド	説明
Authentication attempts:successful 1, failed 0	ポートでのMACアドレス認証の統計情報。これには、認証に成功した回数と失敗した回数が含まれます。
MAC address	アクセスユーザのMACアドレス
Auth state	アクセスユーザの状態 • Authenticated:認証の成功 • Unauthenticated:認証に失敗しました
AP name	AP名
Radio ID	Radio番号
SSID	サービスセット識別子
BSSID	基本サービスセット識別子

1.1.12 display mac-authentication connection

Syntax

display mac-authentication connection [**ap** *ap-name* [**radio** *radio-id*] | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *user-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*:ユーザを認証するために指定された AP にアクセスするすべての MAC アドレスに関する情報を表示します。ap-name は AP の名前です。1~64 文字の文字列で、英数字、アンダースコア、[」 、 「]、 「/」 、 「-」 を使用でき、大文字と小文字が区別されます。このパラメータを指定しない場合、デバイス上のすべての MAC アドレス認証ユーザ情報が表示されます。

radio *radio-id*:指定された Radio にアクセスするすべての MAC アドレス認証ユーザの情報を表示します。radio-id は Radio 番号を表し、デバイスモデルに関連する値の範囲を取ります。このパラメータを指定しない場合、AP のすべての Radio の MAC アドレスがユーザを認証する情報を表示します。このパラメータを指定しない場合、デバイス上のすべての MAC アドレス認証ユーザ情報が表示されます。

slot *slot-number:*クラウドクラスタメンバーデバイスをそのメンバーID で指定します。メンバーデバイスを指定しない場合、このコマンドはすべてのメンバーデバイスのオンライン MAC 認証ユーザに関する情報を表示します。

user-mac *mac-address*:指定した MAC アドレスの MAC アドレス認証ユーザ情報を表示します。ここで、mac-addr はユーザの MAC アドレスで、H-H-H の形式です。このパラメータを指定しない場合、デバイス上のすべての MAC アドレス認証ユーザ情報が表示されます。

user-name *user-name*:指定したユーザ名の MAC アドレス認証ユーザ情報を表示します。ここで、user-name はユーザ名(ドメイン名を含めることができます)を表します。は 1~55 文字の文字列で、大文字と小文字が区別されます。このパラメータを指定しない場合、デバイス上のすべての MAC アドレス認証ユーザ情報が表示されます。

説明

display mac-authentication connection コマンドは、オンラインユーザの MAC アドレス認証の詳細を表示します。

例

#すべての MAC アドレス認証オンラインユーザ情報を表示します。

<Sysname> display mac-authentication connection

```
Total connections: 1
Slot ID: 0
User MAC address            : 0015-e9a6-7cfe
AP name                    : ap1
Radio ID                   : 1
SSID                       : wlan_dot1x_ssid
BSSID                      : 0015-e9a6-7cf0
User name                  : ias
Authentication domain        : 1
Initial VLAN               : 1
Authorization VLAN          : 100
Authorization ACL number     : 3001
Authorization user profile    : N/A
Authorization CAR           : N/A
Authorization URL           : N/A
Authorization IPv6 URL       : N/A
Termination action          : Radius-request
Session timeout last from    : 2023/05/30 17:32:42
Session timeout period       : 86400 s
Online from                : 2023/05/30 11:20:41
Online duration             : 6h 18m 39s
```

表 1-4 display mac-authentication connection コマンドの表示情報の説明

フィールド	説明
Total connections	オンラインMACアドレス認証ユーザ数
User MAC address	ユーザのMACアドレス
Access interface	ユーザのアクセスインタフェース名
AP name	APの名前
Radio ID	RadioのID
SSID	サービスセット識別子
BSSID	ユーザが属する基本サービスセット識別子
Username	ユーザ名
User access state	ユーザのアクセス状態 • Successful:MAC アドレス認証成功とアクセス • Open:存在しないユーザ名または誤ったパスワードを使用してオープン認証を行い、アクセスする
Authentication domain	認証に使用するISPドメインの名前
IPv4 address	ユーザIPv4アドレス ユーザのIPアドレスが取得されていない場合、このフィールドは表示されません。
IPv6 address	ユーザIPv6アドレス ユーザのIPアドレスが取得されていない場合、このフィールドは表示されません。
Initial VLAN	初期VLAN
Authorization untagged VLAN	承認済みuntagged VLAN
Authorization tagged VLAN	承認済みtagged VLAN
Authorization ACL number/name	認可ACLの番号または名前。許可されていないACLの場合はN/A;不正が成功すると、ACL番号の後に「(NOT effective)」と表示されます。
Authorization user profile	認証ユーザのUser profile名

フィールド	説明
Authorization CAR	サーバがユーザCAR属性を承認していない場合、このフィールドはN/Aと表示されます。 サーバがユーザCARプロパティを認可すると、次の4つのフィールドに分割されます。 • Average input rate :bps 単位のアップストリーム平均レート • Peak input rate:bps 単位のアップストリームピーク速度 • Average output rate:bps 単位のダウンストリーム平均レート • Peak output rate:ビット/秒単位の下り最大レート 不正が成功した場合は、(NOT effective)と表示されます。 上下行の平均レートのみが発生する場合、この上下行ピークレートはデフォルトでその平均レートと同じである。アップ/ダウンのピークレートを個別に許可するサーバは現在サポートされていない
Authorization URL	許可されたリダイレクトURL
Termination action	サーバから送信される終了アクションのタイプ: • Default:セッションのタイムアウト時間に達したら、ユーザーを強制的にオフラインにします。 • Radius-Request:セッションタイムアウト時間に達すると MAC アドレス認証を要求ユーザは再認証を行う. ユーザがローカル認証を使用している場合、このフィールドにはDefaultと表示されます。
Session timeout period	サーバから送信されたセッションタイムアウト時間に到達すると、ユーザが存在するセッションは削除され、その後、そのユーザに対して行われたアクションは、Termination actionフィールドの値によって決定される.
Offline detection	ユーザによるオフライン検出のプロパティ: • Ignore (command-configured):コマンドラインでユーザがオフライン検出を行わないように設定します。 • timer (command-configured):コマンドライン設定のオフライン検出時間 • Ignore (server-assigned):RADIUS サーバは、ユーザがオフライン検出を行わないことを許可します。 • timer (server-assigned):RADIUS サーバ認可のオフライン検出時間
Online from	MAC認証ユーザのオンライン時間

フィールド	説明
Online duration	MAC認証ユーザのオンライン時間

1.1.13 dot1x authentication-method

Syntax

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

デフォルト

EAP

View

System view

定義済みユーザロール

network-admin

パラメータ

chap:EAP-Termination モードを有効にし、RADIUS サーバとの CHAP タイプの認証方式をサポートします。

eap:EAP リレー方式を有効にし、クライアントと RADIUS サーバ間のすべてのタイプの EAP 認証方式をサポートします。

pap:EAP 終了モードを有効にし、RADIUS サーバとの間で PAP タイプの認証方式をサポートします。

説明

dot1x authentication-method コマンドを使用して、802.1X システムの認証方式を設定します。

undo dot1x authentication-method コマンドを使用して、デフォルトに戻します。

EAP-Termination モードでは、デバイスは、受信したクライアント EAP メッセージ内のユーザ認証情報を標準の RADIUS メッセージに再カプセル化し、PAP または CHAP 認証方式を使用して RADIUS サーバとの認証対話を完了します。この方式の利点は、既存の RADIUS サーバが基本的に PAP と CHAP 認証をサポートできるため、サーバをアップグレードする必要がないことであるが、設備処理が複雑で、現在は MD5-Challenge タイプの EAP 認証と iNode 802.1X クライアントからの「ユーザ名+パスワード」方式の EAP 認証しかサポートできない。PAP と CHAP の両方の認証方式の詳細については、次のとおりです。

- PAP (Password Authentication Protocol、パスワード認証プロトコル)は、ユーザ名とパスワードを使用してユーザを認証します。PAP は、ネットワーク上でユーザ名

とパスワードを平文で送信することを特徴とし、ネットワーク・セキュリティ要件が比較的低い環境でのみ使用できます。

- CHAP (Challenge Handshake Authentication Protocol 、 Challenge Handshake Authentication Protocol)は、クライアント側とサーバ側の対話型チャレンジ情報を使用してユーザを認証します。ネットワーク上でユーザ名が平文で送信され、パスワードが暗号化テキストで送信されます。CHAP 認証は PAP よりも機密性が高く、より安全です。

EAP リレー方式では、デバイスは受信したクライアント EAP メッセージを直接 RADIUS メッセージの属性フィールドにカプセル化し、 RADIUS サーバに送信して認証を完了する。この方式の利点は、デバイス処理が簡単で、MD5-Challenge、EAP-TLS、PEAP などのような複数のタイプの EAP 認証方式をサポートできるが、サーバ側で対応する EAP 認証方式をサポートする必要があることである。

リモート RADIUS 認証を使用する場合、PAP、CHAP、EAP 認証の最終実装では、RADIUS サーバが適切な PAP、CHAP、EAP 認証方式をサポートする必要があります。

EAP 認証方式を使用する場合、RADIUS スキーマの user-name-format 構成は無効です。user-name-format の説明は、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

例

#EAP-Termination モードを有効にし、RADIUS サーバとの PAP タイプの認証方式をサポートします。

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

関連コマンド

- **display dot1x**

1.1.14 dot1x domain

Syntax

dot1x domain *domain-name*

undo dot1x domain

デフォルト

サービステンプレートで 802.1X ユーザの ISP ドメインが指定されていません。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name:ISP ドメイン名。1~255 文字の文字列で、大文字と小文字は区別されません。

説明

dot1x domain コマンドは、サービステンプレートで 802.1X ユーザの認証ドメインを指定するために使用されます。

undo dot1x domain コマンドを使用して、デフォルトに戻します。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

サービステンプレートからアクセスする 802.1X ユーザは、サービステンプレートで指定された認証ドメイン-->ユーザ名で指定された認証ドメイン-->システムのデフォルト認証ドメインの順に認証ドメインを選択します。

例

#サービステンプレート service1 を設定し、802.1X 認証のドメインに my-domain を使用します。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x domain my-domain
```

1.1.15 dot1x handshake enable

Syntax

dot1x handshake enable

undo dot1x handshake enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x handshake enable コマンドを使用して、802.1X オンラインユーザハンドシェイクを有効にします。

undo dot1x handshake enable コマンドを使用して、802.1X オンラインユーザハンドシェイク機能を無効にします。

802.1X ハンドシェイク機能が有効になると、デバイスは 802.1X 認証済みのオンラインユーザにハンドシェイクメッセージであるユニキャスト EAP-Request/Identity メッセージを定期的に送信して、ユーザのオンライン状態を検出します。ハンドシェイクメッセージ送信の時間間隔は、802.1X ハンドシェークタイマによって制御される(間隔は、コマンド **dot1x timer handshake-period** で設定します。)。ハンドシェイクメッセージを連続して送信した回数が、 802.1X メッセージの最大再送回数(コマンド dot1x retry で設定した最大再送回数)に達してもユーザの応答がなければ、そのユーザに強制的にオフラインにする。

802.1X ハンドシェイクが成功すると、デバイスはユーザに応答しなくなり、一部のクライアントは再認証またはオフラインになります。この機能は状況に応じて設定してください。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

ワイヤレスクライアントによっては、この機能を有効にするとオフラインになる場合があります。クライアントがオフラインになる場合は、この機能を無効にすることをお勧めします。

例

#サービステンプレート service1 で 802.1X オンラインユーザハンドシェイクを有効にします。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x handshake enable
```

関連コマンド

- **dot1x handshake secure enable**
- **dot1x retry (ユーザアクセスと認証-802.1X)**
- **dot1x timer handshake-period (ユーザアクセスと認証-802.1X)**

1.1.16 dot1x handshake secure enable

Syntax

dot1x handshake secure enable

undo dot1x handshake secure enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x handshake secure enable コマンドを使用して、802.1X オンラインユーザのセキュリティハンドシェイクを有効にします。

undo dot1x handshake secure enable コマンドは、802.1X オンラインユーザのセキュリティハンドシェイク機能を無効にするために使用します。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

802.1X Secure Handshake 機能は、802.1X Handshake 機能が有効になっている場合にのみ有効です。

このコマンドは、 802.1X アクセス認証を行いオンライン化に成功したユーザに対してのみ有効である。

例

#サービステンプレート service1 の下で 802.1X オンラインユーザセキュリティハンドシェイク機能を有効にします。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x handshake enable
[Sysname-wlan-st-service1] dot1x handshake secure enable
```

関連コマンド

- **dot1x handshake enable**

1.1.17 dot1x max-user

Syntax

dot1x max-user *count*

undo dot1x max-user

デフォルト

1 つの無線周波数で 1 つの無線サービステンプレートに同時にアクセスできる 802.1X ユーザの数は 512 です。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

count:1 つの無線周波数における 1 つの無線サービステンプレートで同時にアクセスできる最大 802.1 人の X ユーザ数。範囲は 1~512 です。

説明

dot1x max-user コマンドを使用して、1 つの無線周波数で、1 つのサービステンプレートの 802.1X 最大ユーザ数を設定します。

undo dot1x max-user コマンドを使用して、デフォルトに戻します。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

このコマンドを設定すると、1 つの無線周波数で 1 つの無線サービステンプレートに同時にアクセスする 802.1X ユーザの数が最大数を超えると、新しいユーザは拒否されます。

例

#単一無線の設定単一無線サービステンプレート service1 の 802.1X 最大ユーザ数は 500 です。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x max-user 500
```

1.1.18 dot1x re-authenticate enable

Syntax

dot1x re-authenticate enable

undo dot1x re-authenticate enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x re-authenticate enable コマンドは、802.1X の定期的な再認証機能を有効にするために使用します。

undo dot1x re-authenticate enable コマンドは、802.1X 定期再認証機能を無効にするために使用します。

無線サービステンプレートが 802.1X の周期性再認証機能を起動した後、デバイスは system view の下に配置した周期性再認証タイマー(dot1x timer reauth-period)時間間隔によってオンライン 802.1X ユーザに認証を起動し、ユーザ接続状態の変化を検出し、サーバが送信した許可属性(ACL、VLAN、User Profile など)を更新する。

ユーザが 802.1X 認証に成功した後、サーバが Termination action と Session timeout の属性(display dot1x connection)を送信し、Termination action に Radius-Request の値が設定され、Session timeout に 0 以外の値が設定されている場合、デバイスは Session timeout の周期でユーザを再認証し、ユーザのオンライン状態を検出し、許可情報を更新します。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

認証サーバが Terminal action と Session timeout の属性を送信しなかったり、送信した Terminal action の値が Request でない場合、 802.1X 再認証機能を有効にすると、デバイスはすでに在線している 802.1X ユーザに対しても定期的に再認証を開始し、このときの再認証周期は 802.1X 再認証タイマーで構成される。

ワイヤレスクライアントによっては、この機能を有効にするとオフラインになる場合があります。クライアントがオフラインになる場合は、この機能を無効にすることをお勧めします。

例

#サービステンプレート service1 の 802.1X 再認証を有効にします。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] dot1x re-authenticate enable
```

関連コマンド

- **dot1x timer (ユーザアクセスと認証-802.1X)**

1.1.19 dot1x retry

Syntax

dot1x retry *retries*

undo dot1x retry

デフォルト

10 回

View

System view

定義済みユーザロール

network-admin

パラメータ

retries:アクセスユーザに認証要求メッセージを送信する最大試行回数は、 1~10 の範囲である。

説明

dot1x retry コマンドは、デバイスがアクセスユーザに認証要求メッセージを送信する最大回数を設定します。

undo dot1x retry コマンドを実行するとリトライ回数を 2 回に変更します。

アクセスデバイスは、次のいずれかの状況でクライアントに認証要求を再送信します。

- デバイスは、ユーザ名要求タイムアウト間隔内にクライアントから応答を受信しません。タイマは、EAP-Request/Identity パケットに対して **dot1x timer tx-period** コマンドを使用して設定されます。
- デバイスは、クライアントタイムアウト間隔内にクライアントから応答を受信しません。タイマは、EAP-Request/MD5-Challenge パケットに対して **dot1x timer supp-timeout** コマンドを使用して設定されます。

アクセスデバイスは、最大回数の要求送信試行を行っても応答を受信しない場合、要求の再送信を停止します。

🕮 **メモ:**

リトライ回数をデフォルトに戻す場合は **dot1x retry 10** コマンドを実行してください。

例

#アクセスユーザに認証要求メッセージを最大 9 回送信するようにデバイスを設定します。

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

関連コマンド

- **display dot1x**
- **dot1x timer**

1.1.20 dot1x timer

Syntax

dot1x timer { handshake-period *handshake-period-value* **| reauth-period** *reauth-period-value* **| server-timeout** *server-timeout-value* **| supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* **}**

undo dot1x timer { handshake-period | reauth-period | server-timeout | supp-timeout | tx-period }

デフォルト

- ハンドシェイクタイマ:15 秒
- 定期再認証タイマ:3600 秒
- サーバタイムアウトタイマ:100 秒
- クライアントタイムアウトタイマ:2 秒
- ユーザ名要求タイムアウトタイマ：2 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

handshake-period *handshake-period-value*:ハンドシェイクタイマの値。範囲は 5~1024 で、単位は秒です。

reauth-period *reauth-period-value*:周期的再認証タイマの値は、 60~7200 の範囲で、単位は秒である。

server-timeout *server-timeout-value*: 認証サーバのタイムアウトタイマの値で、100~300 の範囲の値をとり、単位は秒である。

supp-timeout *supp-timeout-value*:クライアント認証タイムアウトタイマの値は、 1~120 の範囲で、単位は秒である。

tx-period *tx-period-value*: ユーザ名要求タイムアウトタイマを設定します。設定範囲は 10～120 秒です。

説明

dot1x timer コマンドは、802.1X のタイマパラメータを設定します。

undo dot1x timer コマンドは、指定されたタイマをデフォルトに戻すために使用します。

802.1X 認証プロセスは、次のタイマによって制御されます。

- ハンドシェイクタイマ(handshake-period):このタイマはユーザ認証が成功した後に起動し、デバイス側はこの間隔を周期としてハンドシェーク要求メッセージを送信し、定期的にユーザのオンライン状況を検出する。送信回数を N に設定すると、デバイス側でクライアントからの応答メッセージが N 回連続して受信されない場合、ユーザはオフラインになったと見なされます。
- 周期的再認証タイマ(reauth-period):ポートで周期的再認証機能(コマンド dot1x re-authenticate)が有効になると、デバイス側はこの間隔を周期としてポート上のオンラインユーザに対して再認証を開始する。すでにオンラインになっている 802.1X ユーザの場合は、現在の再認証サイクルが終了し、認証が完了するまで、新しい設定サイクルに従って再認証が行われません。
- 認証サーバタイムアウトタイマ(server-timeout):アクセスデバイスが RADIUS Access-Request パケットを認証サーバに送信したときに開始します。このタイマが

期限切れになっても応答がない場合、802.1X 認証は失敗します。サーバタイムアウトタイマが期限切れになる前に強制ログオフされないようにするには、サーバタイムアウトタイマを次の値の積以下の値に設定します。

- RADIUS scheme view で **retry** コマンドを使用して設定された RADIUS パケット送信の最大試行回数。
- RADIUS scheme view で **timer response-timeout** コマンドを使用して設定された RADIUS サーバ応答タイムアウトタイマ。
  RADIUS メッセージ送信の最大試行回数、RADIUS サーバ応答タイムアウト時間の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

- クライアント認証タイムアウトタイマ(supp-timeout):設備側はクライアントに EAP-Request/MD5 Challenge 要求メッセージを送信した後、設備側はこのタイマを起動し、もしこのタイマが設定した時間内に、設備側はクライアントの応答を受信しなければ、設備側はこのメッセージを再送する。
- ユーザ名要求タイムアウトタイマ（tx-period）:装置が EAP-Request/Identity パケットをクライアントに認証要求の応答として送信するときに開始します。タイマが終了する前に装置が応答を受信しない場合、要求を再送します。認証をアクティブに要求できないクライアントを検出するため、EAP-Request/Identity パケットをネットワーク装置に、設定されたタイマの間隔でマルチキャストします。

通常、ユーザはタイマ値を変更する必要はありません。ただし、特定のネットワーク環境または過酷なネットワーク環境で、このコマンドを使用して対話プロセスを調整できる場合は除きます。

定期的な再認証タイマ以外のタイマは、変更後すぐに有効になります。

🕮 メモ:

supp-timeout と tx-period は **undo** コマンドでデフォルトに戻りません。デフォルトに戻す場合は、それぞれ以下のコマンドを実行してください。
dot1x timer supp-timeout 2
dot1x timer tx-period 2

例

#認証サーバのタイムアウトタイマを 150 秒に設定します。

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

関連コマンド

- **display dot1x**
- **retry (ユーザアクセスと認証/AAA)**
- **timer response-timeout (RADIUS scheme view) (ユーザアクセスと認証/AAA)**

1.1.21 fail-permit enable

Syntax

fail-permit enable [**keep-online**]

undo fail-permit enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

パラメータ

keep-online: 失敗許可機能が動作する際、オンラインのクライアントが切断されるのを防ぎます。

説明

fail-permit enable コマンドは、コマンドは失敗許可機能を有効にします。

undo fail-permit enable コマンドは、失敗許可機能を無効にします。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

このコマンドは、同じサービステンプレートで **fail-permit template** コマンドと同時に設定することはできません。

例

Service template view で失敗許可機能を有効にします。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] fail-permit enable
```

関連コマンド

- **fail-permit template**

1.1.22 fail-permit template

Syntax

fail-permit template

undo fail-permit template

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

fail-permit template コマンドを使用して、バックアップ用サービステンプレートとして指定します。

undo fail-permit template コマンドを使用して、バックアップ用サービステンプレートの指定を解除します。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

このコマンドは、同じサービステンプレートで **fail-permit enable** コマンドと同時に設定することはできません。

例

#現在のサービステンプレートをバックアップ用サービステンプレートとして設定します。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] fail-permit template
```

関連コマンド

- **fail-permit enable**
- **akm mode**

1.1.23 mac-authentication authentication-method

Syntax

mac-authentication authentication-method { **chap** | **pap** }

undo mac-authentication authentication-method

デフォルト

PAP

View

System view

定義済みユーザロール

network-admin

パラメータ

chap:CHAP タイプを使用する認証方式。

pap:PAP タイプを用いた認証方式。

説明

mac-authentication authentication-method コマンドを使用して、MAC アドレス認証に使用する認証方式を設定します。

undo mac-authentication authentication-method コマンドを使用して、デフォルトに戻します。

このコマンドを使用すると、デバイスが MAC アドレス認証を行うときに RADIUS サーバとの間で使用する認証方法を設定できます。PAP および CHAP 認証方式の詳細は、次のとおりです。

- PAP (Password Authentication Protocol、パスワード認証プロトコル)は、ユーザ名とパスワードを使用してユーザを認証します。PAP は、ネットワーク上でユーザ名とパスワードを平文で送信することを特徴とし、ネットワーク・セキュリティ要件が比較的低い環境でのみ使用できます。
- CHAP (Challenge Handshake Authentication Protocol 、 Challenge Handshake Authentication Protocol)は、クライアント側とサーバ側の対話型チャレンジ情報を使用してユーザを認証します。ネットワーク上でユーザ名が平文で送信され、パスワードが暗号化テキストで送信されます。CHAP 認証は PAP よりも機密性が高く、より安全です。

例

#MAC アドレス認証に CHAP 認証方式を使用するようにデバイスを構成します。

```
<Sysname> system-view
[Sysname] mac-authentication authentication-method chap
```

関連コマンド

- **display mac-authentication**

1.1.24 mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

デフォルト

サービステンプレートの MAC アドレスが指定されていないユーザを認証する ISP ドメイン。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name:ISP ドメイン名。1~255 文字の文字列で、大文字と小文字は区別されません。

説明

mac-authentication domain コマンドを使用して、サービステンプレートの MAC アドレスでユーザを認証する ISP ドメインを指定します。

undo mac-authentication domain コマンドを使用して、デフォルトに戻します。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

サービステンプレートからアクセスする MAC アドレス認証ユーザは、サービステンプレートで指定されている ISP ドメイン-->グローバル MAC アドレス ISP ドメイン-->システムのデフォルト ISP ドメインの順に ISP ドメインを選択します。

例

#サービステンプレートの設定 service1 次の MAC アドレス認証ユーザが使用する ISP ドメインは my-domain です。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] mac-authentication domain my-domain
```

1.1.25 mac-authentication max-user

Syntax

mac-authentication max-user *count*

undo mac-authentication max-user

デフォルト

1 つの無線で 1 つの無線サービステンプレートにアクセスできる MAC アドレス認証の最大ユーザ数は 4096 です。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

count:単一無線における単一無線サービステンプレートでの同時アクセスを許可する MAC アドレス認証ユーザの最大数。範囲は 1~4096 です。

説明

mac-authentication max-user コマンドを使用して、1 つの無線周波数で 1 つの無線サービステンプレートの MAC アドレス認証の最大ユーザ数を設定します。

undo mac-authentication max-user コマンドを使用して、デフォルトに戻します。

このコマンドは、サービステンプレートが無効の場合にのみ設定できます。

このコマンドを設定すると、1 つの無線周波数で 1 つの無線サービステンプレートに同時にアクセスする MAC アドレス認証ユーザの数が最大数を超えると、新しいアクセスユーザは拒否されます。

例

#単一無線の設定単一のサービステンプレートでの MAC アドレス認証の最大ユーザ数は 32 です。

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] mac-authentication max-user 32
```

1.1.26 mac-authentication timer (system view)

Syntax

mac-authentication timer server-timeout *server-timeout-value*

undo mac-authentication timer server-timeout

デフォルト

サーバタイムアウトタイマの値は 100 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

server-timeout *server-timeout-value*:サーバタイムアウトタイマを示します。ここで、server-timeout-value はサーバタイムアウトタイマの値であり、 100~300 の範囲の値をとり、単位は秒である。

説明

mac-authentication timer コマンドは、MAC アドレス認証のタイマパラメータを設定します。

undo mac-authentication timer コマンドを使用して、デフォルトに戻します。

サーバタイムアウトタイマ(server-timeout):デバイスと RADIUS サーバ間の接続のタイムアウト時間を設定します。ユーザの認証中に、サーバのタイムアウトタイマが切れるまで、デバイスが RADIUS サーバから応答を受信しない場合、デバイスは適切なポートでそのユーザがネットワークにアクセスできないようにします。server-timeout の値は、デバイスが RADIUS メッセージを送信する最大試行回数(retry)と RADIUS サーバの応答タイムアウト時間(timer response-timeout)の積以下に設定することをお勧めします。server-timeout の値が retry と timer response-timeout の積より大きい場合、server-timeout で設定されたサーバタイムアウト時間に達する前に、ユーザが強制的にオフラインにされる可能性があります。RADIUS メッセージ送信の最大試行回数、RADIUS サーバ応答タイムアウト時間の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

例

#サーバタイムアウトタイマの長さを 150 秒に設定します。

```
<Sysname> system-view
[Sysname] mac-authentication timer server-timeout 150
```

関連コマンド

- **display mac-authentication**
- **retry (ユーザアクセスと認証/AAA)**
- **timer response-timeout (RADIUS scheme view) (ユーザアクセス認証/AAA)**

1.1.27 mac-authentication user-name-format

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*][**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** [**six-section** | **three-section**] | **without-hyphen** } [**lowercase** | **uppercase**]] }

undo mac-authentication user-name-format

デフォルト

ユーザの MAC アドレスをユーザ名とパスワードとして使用します。ここで、文字は小文字で、ハイフン 「-」 は使用しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

fixed:固定ユーザ名アカウントを使用することを示す。

account name:認証のために RADIUS サーバに送信するユーザ名、またはローカルで認証するユーザ名を指定します。name はユーザ名で、大文字と小文字が区別される 1~55 文字の文字列です。@は使用できません。デフォルトは mac です。

password:固定ユーザ名のパスワードを指定します。password パラメータを設定しない場合は、パスワードがありません。

- **cipher**:パスワードを暗号文で設定します。
- **simple**:暗号化されたテキストとして保存されるパスワードを平文で設定します。

string:大文字と小文字を区別するパスワード文字列。平文パスワードは 1~63 文字の文字列、暗号文パスワードは 1~117 文字の文字列である。

mac-address:ユーザの MAC アドレスをユーザ名として使用することを示す。

with-hyphen [**six-section** | **three-section**]:ハイフン 「-」 を使用した MAC アドレス形式。six-section は、xx-xx-xx-xx-xx-xx や XX-XX-XX-XX-XX-XX などの 6 セグメント MAC アドレス形式を表します。three-section は、xxxx-xxxx-xxxx や XXXX-XXXX-XXXX のような 3 分割 MAC アドレス形式を表します。パラメータを指定しない場合、デフォルトは 6 セグメント MAC アドレス形式です。

without-hyphen:xxxxxxxxxxxx など、ハイフン 「-」 を含まない MAC アドレス形式。

lowercase:MAC アドレスの文字は小文字です。

uppercase:MAC アドレスの文字は大文字です。

説明

mac-authentication user-name-format コマンドを使用して、MAC アドレス認証ユーザのアカウントフォーマットを設定します。

undo mac-authentication user-name-format コマンドを使用して、デフォルトに戻します。

指定ユーザの MAC アドレスがユーザ名の場合、 MAC アドレス認証ユーザごとに一意のユーザ名を用いて認証を行うため、安全性は高いが、認証サーバ側に複数の MAC 形式のユーザアカウントを設定する必要がある。

固定ユーザ名を指定すると、ユーザの MAC アドレスに関係なく、すべてのユーザがデバイスで指定された固定ユーザ名とパスワードを ID 情報として使用して認証されます。同じポートで複数のユーザが認証できるため、この場合、ポート上のすべての MAC アドレス認証ユーザは同じ固定ユーザ名アカウントを使用して認証を行い、サーバ側は 1 つのユーザアカウントを設定するだけですべての認証ユーザの認証ニーズを満たすことができ、アクセスクライアントの比較的信頼できるネットワーク環境に適用する。

例

#MAC アドレス認証を設定するユーザ名は abc、パスワードは平文 xyz です。

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc password simple xyz
```

#設定ユーザの MAC アドレスは、ハイフン 「-」 を含まない MAC アドレス形式のユーザ名とパスワードです。ここで、文字は大文字です。

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format mac-address without-hyphen uppercase
```

関連コマンド

- **display mac-authentication**

1.1.28 reset dot1x statistics

Syntax

reset dot1x statistics [**ap** *ap-name* [**radio** *radio-id*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*:指定した AP のすべての 802.1X 統計情報をクリアします。ap-name は AP の名前です。1~64 文字の文字列で、英数字、アンダースコア、[」 、 「]、 「/」 、 「-」 を使用でき、大文字と小文字が区別されます。このパラメータを指定しない場合は、すべての AP の 802.1X 統計情報がクリアされます。

radio *radio-id*:指定した AP のすべての 802.1X 統計情報をクリアします。radio-id は Radio 番号を表し、デバイスモデルに関連する値の範囲を取ります。このパラメータを指定しない場合は、指定した AP のすべての Radio の 802.1X 統計情報がクリアされます。

説明

reset dot1x statistics コマンドは、802.1X の統計情報をクリアするために使用されます。

例

AP 名が ap1 の 802.1X 統計情報をクリアします。

```
<Sysname> reset dot1x statistics ap ap1
```

関連コマンド

- **display dot1x**

1.1.29 reset mac-authentication statistics

Syntax

reset mac-authentication statistics [**ap** *ap-name* [**radio** *radio-id*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

ap *ap-name*:指定した AP のすべての MAC アドレス認証統計情報をクリアします。ap-name は AP の名前です。1~64 文字の文字列で、英数字、アンダースコア、[」 、 「]、「/」 、 「-」 を使用でき、大文字と小文字が区別されます。このパラメータを指定しない場合は、すべての AP の MAC アドレス認証統計情報がクリアされます。

radio *radio-id*:指定した AP のすべての MAC アドレス認証統計情報をクリアします。radio-id は Radio 番号を表し、デバイスモデルに関連する値の範囲を取ります。このパラメータを指定しない場合は、指定した AP のすべての RF アンテナの MAC アドレス認証統計情報がクリアされます。

例

AP 名が ap1 の MAC 認証統計情報をクリアします。

```
<Sysname> reset mac-authentication statistics ap ap1
```

関連コマンド

display mac-authentication

目次

このセクションのページは **13-x-x** です。

2 章 WLAN IP スヌーピング 2-1
2.1 WLAN IP スヌーピング設定コマンド 2-1
2.1.1 client ipv4-snooping arp-learning enable 2-1
2.1.2 client ipv4-snooping dhcp-learning enable 2-2
2.1.3 display wlan statistics client-ip-conflict 2-3
2.1.4 wlan client ip-conflict-detection enable 2-4

2章 WLAN IP スヌーピング

2.1 WLAN IP スヌーピング設定コマンド

2.1.1 client ipv4-snooping arp-learning enable

Syntax

client ipv4-snooping arp-learning enable

undo client ipv4-snooping arp-learning enable

デフォルト

ARP を使用してクライアントの IPv4 アドレスを学習する機能がオンになっています。

View

Service template view

定義済みユーザロール

network-admin

説明

client ipv4-snooping arp-learning enable コマンドを使用すると、ARP を使用してクライアントの IPv 4 アドレスを学習できます。

undo client ipv4-snooping arp-learning enable コマンドは、ARP を使用してクライアントの IPv 4 アドレスを学習する機能を無効にするために使用します。

AP は ARP 方式でクライアント IPv4 アドレスを学習すると、学習したクライアント IPv 4 アドレスとクライアント MAC アドレスを WLAN IP Snooping バインディングテーブルエントリとして記録し、バインディングテーブルエントリを AC に同期させます。

このバインディングテーブルエントリは、主に 802.1 X 認証と MAC アドレス認証のユーザ課金に使用されます。

例

#ARP を使用してクライアントの IPv 4 アドレスを学習する機能を無効にします。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] undo client ipv4-snooping arp-learning enable

2.1.2 client ipv4-snooping dhcp-learning enable

Syntax

client ipv4-snooping dhcp-learning enable

undo client ipv4-snooping dhcp-learning enable

デフォルト

DHCP によるクライアント IPv4 アドレスの学習機能が有効になっています。

View

Service template view

定義済みユーザロール

network-admin

説明

client ipv4-snooping dhcp-learning enable コマンドは、DHCP によるクライアント IPv 4 アドレスの学習を有効にするために使用します。

undo client ipv4-snooping dhcp-learning enable コマンドは、DHCP ラーニングクライアント IPv 4 アドレス機能を無効にするために使用します。

AP はクライアント IPv4 アドレスを DHCPv4 で学習すると、学習したクライアント IPv4 アドレスとクライアント MAC アドレスを WLAN IP Snooping バインディングテーブルエントリとして記録し、同期バインディングテーブルエントリを AC に渡す。

このバインディングテーブルエントリは、主に 802.1X 認証と MAC アドレス認証のユーザ課金に使用されます。

例

#DHCP ラーニングクライアント IPv4 アドレス機能をオフにします。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] undo client ipv4-snooping dhcp-learning enable

2.1.3 display wlan statistics client-ip-conflict

> 🕮 **メモ：**
> このコマンドは、ソフトウェアバージョン 9.6.05c を含む以降のソフトウェアからサポートしています。

Syntax

display wlan statistics client-ip-conflict

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan statistics client-ip-conflict コマンドは、IP アドレスが競合しているクライアントの統計を表示します。

例

IP アドレスが競合しているクライアントの統計を表示します。

<AC> display wlan statistics client-ip-conflict

```
IP            New-MAC/APID           Old-MAC/APID     Time
192.168.1.1    a4c1-5b79-fa5b/1     1111-e121-ff00/2     03-22 10:00:00
192.168.1.2    22d3-c5b7-a4b5/2     00a3-02f8-0577/1     03-22 10:01:00
```

表 2-1 コマンド出力

フィールド	説明
IP	クライアントが取得した競合しているIPアドレス
New-MAC/APID	新しいクライアントのMACアドレスと、そのクライアントがオンラインになったAPのID
Old-MAC/APID	古いクライアントのMACアドレスと、そのクライアントが関連付けられているAPのID
Time	クライアントが競合するIPアドレスを取得した時間

2.1.4 wlan client ip-conflict-detection enable

🕮 メモ：

undo wlan client ip-conflict-detection enable 実行時に IP アドレス競合検出された IP アドレスがある場合は、そのクライアントのキャッシュ情報がクリアされるまで、その IP アドレスの競合検出は行いません。クライアントのキャッシュ情報の保持時間は、client cache aging-time コマンドで設定した時間（初期値は 180 秒）です。

Syntax

wlan client ip-conflict-detection enable

undo wlan client ip-conflict-detection enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

network-operator

説明

wlan client ip-conflict-detection enable コマンドは、IP アドレス競合検出機能を有効にします。

undo wlan client ip-conflict-detection enable コマンドは、IP アドレス競合検出機能を無効にします。

この機能により、システムはオンライン要求したクライアントと既にオンライン中のクライアントの間で IP アドレスの競合を検出することができます。システムはオンライン要求したクライアントと同じ IP アドレスを使用しているオンライン中のクライアントをログオフし、そのクライアント用に IP アドレス競合のエントリを作成します。クライアントのキャッシュが期限切れになるか、クライアントの IP アドレスが変更されると、システムはそのクライアントの IP アドレス競合エントリを削除します。

例

IP アドレス競合検出を無効にします。

<AC> system-view

[AC] undo wlan client ip-conflict-detection enabl

目次

このセクションのページは **13-x-x** です。

3 章 AAA 3-1
3.1 AAA 設定コマンド 3-1
3.1.1 aaa session-limit 3-1
3.1.2 accounting default 3-2
3.1.3 accounting lan-access 3-3
3.1.4 accounting login 3-4
3.1.5 authentication default 3-6
3.1.6 authentication lan-access 3-7
3.1.7 authentication login 3-9
3.1.8 authorization command 3-10
3.1.9 authorization default 3-11
3.1.10 authorization lan-access 3-13
3.1.11 authorization login 3-14
3.1.12 display domain 3-16
3.1.13 domain 3-23
3.1.14 domain default enable 3-24
3.1.15 local-server log change-password-prompt 3-25
3.1.16 nas-id 3-27
3.1.17 state (ISP domain view) 3-27
3.2 ローカルユーザ構成コマンド 3-29
3.2.1 access-limit 3-29
3.2.2 authorization-attribute (Local user view/user group view) 3-30
3.2.3 bind-attribute 3-33
3.2.4 description 3-35
3.2.5 display local-user 3-35
3.2.6 display user-group 3-39
3.2.7 group 3-41
3.2.8 local-user 3-42
3.2.9 password (Device management user view) 3-44
3.2.10 password (Network access user view) 3-45
3.2.11 service-type (Local user view) 3-46
3.2.12 state (Local user view) 3-47
3.2.13 user-group 3-48
3.3 RADIUS 設定コマンド 3-49
3.3.1 accounting-on enable 3-49
3.3.2 data-flow-format (RADIUS scheme view) 3-50

3.3.3 display radius scheme 3-52
3.3.4 display radius statistics 3-58
3.3.5 display stop-accounting-buffer (for RADIUS) 3-59
3.3.6 key (RADIUS scheme view) 3-61
3.3.7 nas-ip (RADIUS scheme view) 3-62
3.3.8 primary accounting (RADIUS scheme view) 3-64
3.3.9 primary authentication (RADIUS scheme view) 3-65
3.3.10 radius dscp 3-67
3.3.11 radius nas-ip 3-68
3.3.12 radius scheme 3-70
3.3.13 radius-server test-profile 3-71
3.3.14 reauthentication server-select 3-72
3.3.15 reset radius statistics 3-73
3.3.16 reset stop-accounting-buffer (for RADIUS) 3-73
3.3.17 retry 3-74
3.3.18 retry realtime-accounting 3-75
3.3.19 retry stop-accounting (RADIUS scheme view) 3-77
3.3.20 secondary accounting (RADIUS scheme view) 3-78
3.3.21 secondary authentication (RADIUS scheme view) 3-80
3.3.22 snmp-agent trap enable radius 3-82
3.3.23 state primary 3-83
3.3.24 state secondary 3-85
3.3.25 stop-accounting-buffer enable (RADIUS scheme view) 3-86
3.3.26 timer quiet (RADIUS scheme view) 3-87
3.3.27 timer realtime-accounting (RADIUS scheme view) 3-88
3.3.28 timer response-timeout (RADIUS scheme view) 3-89
3.3.29 user-name-format (RADIUS scheme view) 3-91
3.4 EAP プロファイル設定コマンド 3-92
3.4.1 ca-file 3-92
3.4.2 certificate-file 3-93
3.4.3 eap-profile 3-94
3.4.4 method 3-95
3.4.5 private-key-file 3-96
3.4.6 private-key-password 3-97
3.5 RADIUS サーバ設定コマンド 3-98
3.5.1 display radius-server active-client 3-98
3.5.2 display radius-server active-eap-profile 3-99
3.5.3 display radius-server active-user 3-100
3.5.4 radius-server activate 3-101
3.5.5 radius-server client 3-102
3.5.6 radius-server deactivate 3-103
3.5.7 radius-server eap-profile 3-104

3章 AAA

3.1 AAA設定コマンド

3.1.1 aaa session-limit

Syntax

aaa session-limit { **ftp** | **http** | **https** | **ssh** | **telnet** } *max-sessions*

undo aaa session-limit { **ftp** | **http** | **https** | **ssh** | **telnet** }

デフォルト

同時オンラインの各タイプの最大ユーザ接続数は 32 である。

View

System view

定義済みユーザロール

network-admin

パラメータ

ftp:FTP ユーザを表す。

http:HTTP ユーザを表します。

https:HTTPS ユーザを表します。

ssh:SSH ユーザを示します。

telnet:Telnet ユーザを表します。

max-sessions:同時オンラインが許可されるユーザ接続の最大数は、 SSH/Telnet ユーザでは 132, FTP/HTTP/HTTPS ユーザでは 1~64 の範囲である。

説明

aaa session-limit コマンドは、指定されたログイン方法でデバイスにログインし、同時にオンラインになるユーザの最大接続数を設定します。

undo aaa session-limit コマンドは、指定されたログイン方法でオンラインになっているユーザ接続の最大数をデフォルトに戻すために使用します。

このコマンドを設定すると、指定したタイプのアクセスユーザのユーザ数が現在設定されている最大接続数を超えると、新しいアクセス要求は拒否されます。

HTTP/HTTPS ユーザの場合、異なる上位アプリケーションのユーザ接続の最大数は個別に制限されます。たとえば、同時オンライン HTTP 最大ユーザ接続数を 20 に設定する

と、HTTP ベースの RESTful ユーザ、Web ユーザ、NETCONF ユーザの最大接続数はすべて 20 になります。

例

#同時オンライン FTP ユーザ接続の最大数を 4 に設定します。

<Sysname> system-view
[Sysname] aaa session-limit ftp 4

3.1.2 accounting default

Syntax

accounting default { **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting default

デフォルト

現在の ISP ドメインのデフォルトの課金方法は local です。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカルチャージ。

none:課金されません。

radius-scheme *radius-scheme-name*:RADIUS スキーマを指定します。ここで、*radius-scheme-name* は RADIUS スキーマ名を表し、1~32 文字の文字列であり、大文字と小文字は区別されません。

説明

accounting default コマンドは、現在の ISP ドメインのデフォルトの課金方法を設定します。

undo accounting default コマンドを使用して、デフォルトの状態を復元します。

現在の ISP ドメインのデフォルトの課金方式は、そのドメイン内の特定の課金方式が指定されていないすべてのアクセスユーザに対して有効であるが、特定のタイプのユーザが指定された課金方式をサポートしていない場合、そのようなユーザに対しては有効ではない。

ローカル課金はローカルユーザのコネクション数管理を支援するためだけのものであり、実際の課金に関する統計機能はない。

複数の代替請求方法を指定して、現在の請求方法が無効な場合に、構成された順序で代替方法を使用して請求を完了することができます。例えば、radius-scheme radius-scheme-name local none は、RADIUS 課金が先に行われ、RADIUS 課金が無効であればローカル課金が行われ、ローカル課金も無効であれば課金が行われないことを示す。無効なリモート課金とは、指定された課金プランが存在しない、課金メッセージの送信に失敗した、またはサーバが応答しないことを意味します。無効なローカル課金は、対応するローカルユーザ設定が見つからないことを意味します。

ローカル認証方式が主認証方式として採用され、代替認証方式が設定される時、AAA ローカル課金処理プロセスが異常である或はローカルユーザが設定されない情況で、ユーザローカル認証が失敗した後、代替認証方式を使用して認証を試みて、その他の情況では認証方式を転換しなくて、直接に認証失敗とみなす。

例

#ISP ドメイン test の下で、RADIUS シナリオ rd を使用して課金するようにデフォルトの課金方法を設定し、代替の課金方法として local を使用します。

<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] accounting default radius-scheme rd local

関連コマンド

local-user

radius scheme

3.1.3 accounting lan-access

Syntax

accounting lan-access { **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting lan-access

デフォルト

LAN ユーザの ISP ドメインのデフォルトの課金方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカルチャージ。

none:課金されません。

radius-scheme *radius-scheme-name*:RADIUS スキーマを指定します。ここで、*radius-scheme-name* は RADIUS スキーマ名を表し、1~32 文字の文字列であり、大文字と小文字は区別されません。

説明

accounting lan-access コマンドは、現在の ISP ドメインのデフォルトの課金方法を設定します。

undo accounting lan-access コマンドを使用して、デフォルトの状態を復元します。

1 つのプライマリアカウンティング方式と複数のバックアップアカウンティング方式を指定できます。

プライマリ方式が無効な場合、デバイスはバックアップ方式を順番に使用しようとします。たとえば、**accounting lan-access radius-scheme** *radius-scheme-name* **local none** コマンドは、プライマリ RADIUS アカウンティング方式と 2 つのバックアップ方式 (ローカルアカウンティングと非アカウンティング) を指定します。デバイスはデフォルトで RADIUS アカウンティングを実行し、RADIUS サーバが無効な場合はローカルアカウンティングを実行します。前述の両方の方式が無効な場合、デバイスはアカウンティングを実行しません。

リモートアカウンティング方式は、次の状況では無効です。

指定されたアカウンティング方式が存在しません。

デバイスがアカウンティング要求パケットを送信できません。

デバイスがアカウンティングサーバからアカウンティング応答パケットを受信しません。

デバイスが一致するローカルユーザ設定を検出できない場合、ローカルアカウンティング方式は無効です。

例

#ISP ドメイン test の下で、RADIUS シナリオ rd を使用して課金するようにデフォルトの課金方法を設定し、代替の課金方法として local を使用します。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] accounting lan-access radius-scheme rd local
```

関連コマンド

local-user

radius scheme

3.1.4 accounting login

Syntax

accounting login { **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting login

デフォルト

login ユーザは、現在の ISP ドメインのデフォルトの課金方法を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカルチャージ。

none:課金されません。

radius-scheme *radius-scheme-name*:RADIUS スキーマを指定します。ここで、*radius-scheme-name* は RADIUS スキーマ名を表し、1~32 文字の文字列であり、大文字と小文字は区別されません。

説明

accounting login コマンドは、login ユーザの課金方法を設定するために使用します。

undo accounting login コマンドを使用して、デフォルトの状態を復元します。

FTP、SFTP、および SCP タイプの login ユーザに対する課金はサポートされていません。

複数の代替請求方法を指定できます。現在の課金方法が無効な場合は、設定された順序で別の方法を使用して課金を実行します。例えば、radius-scheme radius-scheme-name local none は、RADIUS 課金が先に行われ、RADIUS 課金が無効であればローカル課金が行われ、ローカル課金も無効であれば課金が行われないことを示す。無効なリモート課金とは、指定された課金プランが存在しない、課金メッセージの送信に失敗した、またはサーバが応答しないことを意味します。無効なローカル課金は、対応するローカルユーザ設定が見つからないことを意味します。

ローカル認証方式が主認証方式として採用され、代替認証方式が設定される時、AAA ローカル課金処理プロセスが異常である或はローカルユーザが設定されない情況で、ユーザローカル認証が失敗した後、代替認証方式を使用して認証を試みて、その他の情況では認証方式を転換しなくて、直接に認証失敗とみなす。

例

#ISP ドメイン test の下で、login ユーザのための請求方法を local 設定して下さい。

```
<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] accounting login local
```

#ISP ドメイン test で、login ユーザが RADIUS シナリオ rd を使用して課金するように設定し、local を別の課金方法として使用します。

<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] accounting login radius-scheme rd local

関連コマンド

accounting default

local-user

radius scheme

3.1.5 authentication default

Syntax

authentication default { **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication default

デフォルト

現在の ISP ドメインのデフォルトの認証方式は local です。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカル認証。

none:認証は行われません。

radius-scheme radius-scheme-name:RADIUS スキーマを指定します。ここで、radius-scheme-name は RADIUS スキーマ名を表し、1~32 文字の文字列であり、大文字と小文字は区別されません。

🕮 **メモ**:

"none"を指定した場合、認証は行われませんが、認証シーケンスとの兼ね合いにより、クライアントが認証に成功するかどうかは、クライアントの仕様に依存します。

説明

authentication default コマンドを使用して、現在の ISP ドメインのデフォルトの認証方式を設定します。

undo authentication default コマンドは、をデフォルトに戻すために使用します。

現在の ISP ドメインのデフォルトの認証方式は、そのドメイン内の特定の認証方式を指定していないすべてのアクセスユーザに有効ですが、特定のタイプのユーザが指定された認証方式をサポートしていない場合、そのタイプのユーザには有効になりません。

複数の代替認証方式を指定できます。現在の認証方式が無効な場合は、設定された順序で代替認証方式を使用して認証を完了します。たとえば、 radius-scheme radius-scheme-name local none は、 RADIUS 認証を先に行い、 RADIUS 認証が無効であればローカル認証を行い、ローカル認証も無効であれば認証を行わないことを表す。無効なリモート認証とは、指定された認証スキームが存在しないか、認証メッセージの送信に失敗したか、サーバが応答しなかったことを指す。無効なローカル認証とは、対応するローカルユーザ設定が見つからないことです。

ローカル認証方式が主認証方式として採用され、代替認証方式が設定される時、AAA ローカル認証処理プロセスが異常である或はローカルユーザが設定されない情況で、ユーザローカル認証が失敗した後、代替認証方式を使用して認証を試みて、その他の情況では認証方式を転換しなくて、直接に認証失敗とみなす。

例

#ISP ドメイン test の下で、認証に RADIUS 方式 rd を使用し、代替認証方式として local を使用するようにデフォルト認証方式を構成します。

<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] authentication default radius-scheme rd local

関連コマンド

local-user

radius scheme

3.1.6 authentication lan-access

Syntax

authentication lan-access { **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication lan-access

デフォルト

LAN ユーザの ISP ドメインのデフォルトの認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカル認証。

none:認証は行われません。

radius-scheme radius-scheme-name:RADIUS スキーマを指定します。ここで、radius-scheme-name は RADIUS スキーマ名を表し、1~32 文字の文字列であり、大文字と小文字は区別されません。

説明

authentication default コマンドを使用して、現在の ISP ドメインのデフォルトの認証方式を設定します。

undo authentication default コマンドは、をデフォルトに戻すために使用します。

1 つのプライマリ認証方式と複数のバックアップ認証方式を指定できます。

プライマリ認証方式が無効な場合、デバイスはバックアップ方式を順番に使用しようとします。たとえば、**authentication lan-access radius-scheme** *radius-scheme-name* **local none** コマンドは、プライマリ RADIUS 認証方式と 2 つのバックアップ方式（ローカル認証と認証なし）を指定します。デバイスはデフォルトで RADIUS 認証を実行し、RADIUS サーバが無効な場合はローカル認証を実行します。前述の方式が両方とも無効な場合、デバイスは認証を実行しません。

リモート認証方式は、次の状況では無効です。

- 指定された認証方式が存在しません。
- デバイスが認証要求パケットを送信できません。
- デバイスが認証サーバから認証応答パケットを受信しません。

デバイスが一致するローカルユーザ設定を検出できない場合、ローカル認証方式は無効です。

プライマリ認証方式がローカルの場合、次のルールがユーザの認証に適用されます。

- デバイスは、次のいずれかの理由でローカル認証が無効な場合にのみ、バックアップ認証方式を順番に使用します。
  - ローカル認証プロセスで例外が発生しました。
  - デバイス接続が終了したか、ユーザアカウントがデバイスで設定されていません。
- 他の理由でローカル認証が無効な場合、デバイスはバックアップ認証方式に切り替えません。ユーザの認証が失敗しました。

例

#ISP ドメイン test の下で、認証に RADIUS 方式 rd を使用し、代替認証方式として local を使用するようにデフォルト認証方式を構成します。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access radius-scheme rd local
```

関連コマンド

local-user

radius scheme

3.1.7 authentication login

Syntax

authentication login { **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **local** [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication login

デフォルト

login ユーザは、現在の ISP ドメインのデフォルトの認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカル認証。

none:認証は行われません。

radius-scheme *radius-scheme-name*:RADIUS スキーマを指定します。ここで、radius-scheme-name は RADIUS スキーマ名を表し、1~32 文字の文字列であり、大文字と小文字は区別されません。

説明

authentication login コマンドは、login ユーザの認証方式を設定するために使用します。

undo authentication login コマンドを使用して、デフォルトの状態を復元します。

複数の代替認証方式を指定できます。現在の認証方式が無効な場合は、設定された順序で代替認証方式を使用して認証を完了します。たとえば、 radius-scheme radius-scheme-name local none は、 RADIUS 認証を先に行い、 RADIUS 認証が無効であればローカル認証を行い、ローカル認証も無効であれば認証を行わないことを表す。無効なリモート認証とは、指定された認証スキームが存在しないか、認証メッセージの送信に失敗したか、サーバが応答しなかったことを指す。無効なローカル認証とは、対応するローカルユーザ設定が見つからないことです。

ローカル認証方式が主認証方式として採用され、代替認証方式が設定される時、AAA ローカル認証処理プロセスが異常である或はローカルユーザが設定されない情況で、ユーザローカル認証が失敗した後、代替認証方式を使用して認証を試みて、その他の情況では認証方式を転換しなくて、直接に認証失敗とみなす。

例

#ISP ドメイン test の下で、login ユーザのための認証方式を local 設定して下さい。

<Sysname> system-view

[Sysname] domain name test

[Sysname-isp-test] authentication login local

#ISP ドメイン test で、RADIUS スキーム rd を使用して login ユーザを認証し、代替認証方法として local を使用するように設定します。

<Sysname> system-view

[Sysname] domain name test

[Sysname-isp-test] authentication login radius-scheme rd local

関連コマンド

authentication default

local-user

radius scheme

3.1.8 authorization command

Syntax

authorization command { **local** [**none**] | **none** }

undo authorization command

デフォルト

コマンドライン認証は、現在の ISP ドメインのデフォルトの認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカル認証。

none:許可されていません。ユーザがロールで許可されているコマンドを実行する場合、認証サーバのチェックを受ける必要はありません。

説明

authorization command コマンドを使用して、コマンドライン認証方式を設定します。

undo authorization command コマンドを使用して、デフォルトの状態を復元します。

コマンドライン認証では、ユーザが実行するすべてのコマンドが認証サーバによって検査され、認証に成功したコマンドのみが許可されます。ユーザがログインした後に実行できるコマンドは、ログイン認証されたユーザの役割とコマンドライン認証されたユーザの役割の両方によって制限されます。つまり、実行できるコマンドラインは、ログイン認証されたユーザの役割とコマンドライン認証されたユーザの役割の両方で許可されている場合にのみ実行できます。コマンドラインの承認機能では、ロール内のアクセス権限規則を使用してコマンドラインのアクセス権限チェックを実行するだけで、リソース制御ポリシーなどの他のアクセス権限チェックは行わないことに注意してください。

ローカルコマンドラインを使用してユーザを認可する場合、デバイスは、ユーザがデバイスにログインしたときに入力したユーザ名に対応するローカルユーザ構成に基づいてユーザが入力したコマンドをチェックし、ローカルユーザで構成された認可ユーザの役割によって許可されたコマンドのみを実行できます。

例

#ISP ドメイン test で、コマンドライン認証方式を local に設定します。

```
<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] authorization command local
```

関連コマンド

command authorization (基本機能/ログイン管理)

local-user

3.1.9 authorization default

Syntax

authorization default { **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization default

デフォルト

現在の ISP ドメインのデフォルトの認証方式は local です。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカル認証。

none:許可されていません。アクセスデバイスは、許可情報を要求せず、ユーザが使用できる操作およびユーザが使用を許可されるネットワークサービスを許可しない。この時点で、認証された Login ユーザ(Console または Telnet、FTP/SFTP/SCP を介してデバイスにアクセスするユーザ)には、システムによって与えられるデフォルトのユーザロール level-0 のみが与えられます。ここで、FTP/SFTP/SCP ユーザの作業ディレクトリはデバイスのルートディレクトリですが、アクセス権はありません。認証された非 Login ユーザは、ネットワークに直接アクセスできます。ユーザロール色 level-0 の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。

radius-scheme *radius-scheme-name*:RADIUS スキーマを指定します。ここで、radius-scheme-name は RADIUS スキーマ名を表し、1~32 文字の文字列であり、大文字と小文字は区別されません。

説明

authorization default コマンドは、現在の ISP ドメインのデフォルトの認証方式を設定します。

undo authorization default コマンドを使用して、デフォルトの状態を復元します。

現在の ISP ドメインのデフォルトの認証方式は、特定の認証方式が指定されていないドメイン内のすべてのアクセスユーザに有効ですが、特定のタイプのユーザが指定された認証方式をサポートしていない場合、そのタイプのユーザには有効になりません。

ISP ドメインでは、RADIUS 認証プロセスは、設定されている認証および認証方式で同じ RADIUS スキームが参照されている場合にのみ有効になります。

複数の代替認証方式を指定できます。現在の認証方式が無効な場合は、設定された順序で代替認証方式を使用して認証を完了します。たとえば、radius-scheme radius-scheme-name local none は、最初に RADIUS が許可され、RADIUS が無効な場合はローカルが許可され、ローカルも無効な場合は許可されないことを意味します。無効なリモート認証とは、指定された認証スキームが存在しないか、認証メッセージの送信に失敗したか、サーバが応答しなかったかのいずれかです。無効なローカル認可は、対応するローカルユーザ設定が見つからないことを意味します。

ローカル認証方式が主認証方式として採用され、代替認証方式が設定された場合、AAA ローカル認証処理プロセスが異常であるか、またはローカルユーザが設定されていない場合に限り、ユーザのローカル認証が失敗した後に代替認証が試みられ、その他の場合には認証方式が変換されず、認証が失敗したと見なされる。

例

#ISP ドメイン test の下で、RADIUS シナリオ rd を使用して認証するようにデフォルトの認証方式を設定し、代替認証方式として local を使用します。

```
<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] authorization default radius-scheme rd local
```

関連コマンド

local-user

radius scheme

3.1.10 authorization lan-access

Syntax

authorization lan-access { **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization lan-access

デフォルト

LAN ユーザの ISP ドメインのデフォルトの認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカル認証。

none:許可されていません。アクセスデバイスは、許可情報を要求せず、ユーザが使用できる操作およびユーザが使用を許可されるネットワークサービスを許可しない。この時点で、認証された Login ユーザ(Console または Telnet、FTP/SFTP/SCP を介してデバイスにアクセスするユーザ)には、システムによって与えられるデフォルトのユーザロール level-0 のみが与えられます。ここで、FTP/SFTP/SCP ユーザの作業ディレクトリはデバイスのルートディレクトリですが、アクセス権はありません。認証された非 Login ユーザは、ネットワークに直接アクセスできます。ユーザロール色 level-0 の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。

radius-scheme *radius-scheme-name*:RADIUS スキーマを指定します。ここで、radius-scheme-name は RADIUS スキーマ名を表し、1~32 文字の文字列であり、大文字と小文字は区別されません。

説明

authorization lan-access コマンドは、現在の ISP ドメインのデフォルトの認証方式を設定します。

undo authorization lan-access コマンドを使用して、デフォルトの状態を復元します。

1 つのプライマリ認証方式と複数のバックアップ認証方式を指定できます。

プライマリ認証方式が無効な場合、デバイスはバックアップ方式を順番に使用しようとします。たとえば、**authentication lan-access radius-scheme** *radius-scheme-name* **local none** コマンドは、プライマリ RADIUS 認証方式と 2 つのバックアップ方式 (ローカル認証と認証なし) を指定します。デバイスはデフォルトで RADIUS 認証を実行し、RADIUS サーバが無効な場合はローカル認証を実行します。前述の方式が両方とも無効な場合、デバイスは認証を実行しません。

リモート認証方式は、次の状況では無効です。

指定された認証方式が存在しません。

デバイスが認証要求パケットを送信できません。

デバイスが認証サーバから認証応答パケットを受信しません。

デバイスが一致するローカルユーザ設定を検出できない場合、ローカル認証方式は無効です。

プライマリ認証方式がローカルの場合、次のルールがユーザの認証に適用されます。

- デバイスは、次のいずれかの理由でローカル認証が無効な場合にのみ、バックアップ認証方式を順番に使用します。
  - ローカル認証プロセスで例外が発生しました。
  - デバイス接続が終了したか、ユーザアカウントがデバイスで設定されていません。
- 他の理由でローカル認証が無効な場合、デバイスはバックアップ認証方式に切り替えません。ユーザの認証が失敗しました。

例

#ISP ドメイン test の下で、RADIUS シナリオ rd を使用して認証するようにデフォルトの認証方式を設定し、代替認証方式として local を使用します。

```
<Sysname> system-view
[Sysname] domain test
[Sysname-isp-test] authentication lan-access radius-scheme rd local
```

関連コマンド

local-user

radius scheme

3.1.11 authorization login

Syntax

authorization login { **local** [**radius-scheme** *radius-scheme-name*] * [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization login

デフォルト

login ユーザは、現在の ISP ドメインのデフォルトの認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local:ローカル認証。

none:許可されていません。アクセスデバイスは、許可情報を要求せず、ユーザが使用できる操作およびユーザが使用を許可されるネットワークサービスを許可しない。この時点で、認証された Login ユーザ(Console または Telnet、FTP/SFTP/SCP を介してデバイスにアクセスするユーザ)には、システムによって与えられるデフォルトのユーザロール level-0 のみが与えられます。ここで、FTP/SFTP/SCP ユーザの作業ディレクトリはデバイスのルートですが、アクセス権はありません。QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。

radius-scheme *radius-scheme-name*:RADIUS スキーマを指定します。ここで、radius-scheme-name は RADIUS スキーマ名を表し、1~32 文字の文字列であり、大文字と小文字は区別されません。

説明

authorization login コマンドは、login ユーザの認証方式を設定するために使用します。

undo authorization login コマンドを使用して、デフォルトの状態を復元します。

ISP ドメインでは、RADIUS 認証プロセスは、設定されている認証および認証方式で同じ RADIUS スキームが参照されている場合にのみ有効になります。

複数の代替認証方式を指定できます。現在の認証方式が無効な場合は、設定された順序で代替認証方式を使用して認証を完了します。たとえば、radius-scheme radius-scheme-name local none は、最初に RADIUS が許可され、RADIUS が無効な場合はローカルが許可され、ローカルも無効な場合は許可されないことを意味します。無効なリモート認証とは、指定された認証スキームが存在しないか、認証メッセージの送信に失敗したか、サーバが応答しなかったかのいずれかです。無効なローカル認可は、対応するローカルユーザ設定が見つからないことを意味します。

ローカル認証方式が主認証方式として採用され、代替認証方式が設定された場合、AAA ローカル認証処理プロセスが異常であるか、またはローカルユーザが設定されていない場合に限り、ユーザのローカル認証が失敗した後に代替認証が試みられ、その他の場合には認証方式が変換されず、認証が失敗したと見なされる。

例

#ISP ドメイン test の下で、login ユーザのための認証方式を local 設定して下さい。

<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] authorization login local

#ISP ドメイン test で、RADIUS シナリオ rd を使用して login ユーザを認証し、代替認証方法として local を使用するように設定します。

<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] authorization login radius-scheme rd local

関連コマンド

authorization default

local-user

radius scheme

3.1.12 display domain

Syntax

display domain [*isp-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

isp-name:ISP ドメイン名。1~255 文字の文字列で、大文字と小文字は区別されません。指定しない場合は、すべての ISP ドメインを表します。

説明

display domain コマンドは、すべての ISP ドメインまたは指定された ISP ドメインの構成情報を表示します。

例

#システム内のすべての ISP ドメインの構成情報を表示します。

<Sysname> display domain
Total 2 domains

Domain:system
Current state:Active
State configuration:Active
Default authentication scheme:Local
Default authorizationscheme:Local
Default accountingscheme:Local
Accounting start failure action:Online
Accounting update failure action:Online
Accounting quota out policy:Offline
Send accounting update:Yes
ITA service policy:ita 1
Service type:HSI
Session time:Exclude idle time
DHCPv6-follow-IPv6CP timeout:Not configured
Dual-stack accounting method:Merge
NAS-ID:N/A
Web server URL:Not configured
Web server URL parameters:Not configured
Web server IPv4 address:Not configured
Web server IPv6 address:Not configured
Authorization attributes:
Idle cut:Disabled
IGMP access limit:4
MLD access limit:4

Domain:dm
Current state:Active
State configuration:Blocked during specific time ranges
Time ranges:
t 1
t 2
Online-user logoff:Disabled
Loginauthentication scheme:RADIUS=rad
Loginauthorizationscheme:HWTACACS=hw
Superauthentication scheme:RADIUS=rad
Command authorizationscheme:HWTACACS=hw
LAN access authentication scheme:RADIUS=r 4
Portalauthentication scheme:LDAP=ldp
IPoEauthentication scheme:RADIUS=rad, Local, None
Default authentication scheme:RADIUS=rad, Local, None
Default authorizationscheme:Local
Default accountingscheme:なし
Accounting start failure action:Online

Accounting update failure action:Online
Accounting quota out policy:Offline
ITA service policy:ita 1
Service type:HSI
Session time:Include idle time
Dual-stack accounting method:Merge
NAS-ID:test
Web server URL:Not configured
Web server URL parameters:Not configured
Web server IPv4 address:Not configured
Web server IPv6 address:Not configured
Authorization attributes:
Idle cut :Enabled
Idle timeout:2 minutes
Flow:10240 bytes
Traffic direction:Both
IP pool:appy
User profile:test
Session group profile:abc
Inbound CAR:CIR 64000 bps PIR 640000 bps
Outbound CAR:CIR 64000 bps PIR 640000 bps
ACL number:3000
User group:ugg
IPv6 prefix:1::1/34
IPv6 pool:ipv6pool
Primary DNS server:6.6.6.6
Secondary DNS server:3.6.2.3
URL:http://test
IGMP access limit:4
MLD access limit:4

Default domain name:system

表 3-1 display domain コマンドの表示情報の説明

フィールド	説明
Total 2 domains	合計2つのISPドメイン
Domain	ISPドメイン名
Current state	次の値を含むISPドメインの現在のステータス。 • Blocked:ブロック状態 • Active:アクティブステータス

フィールド	説明
State configuration	ISPドメインのステータス設定。次の値が含まれます。 • Active:アクティブステータス • Blocked during specific time ranges:指定した時間ブロックされています • Blocked:ブロック状態
Time ranges	ISPドメインがブロックされている期間の名前
Online-user logoff	ブロックされた状態のISPは、次の値を含むオフライン機能を強制します。 • Enabled:オン • Disabled:オフ
Default authentication scheme	デフォルトの認証スキーム
Default authorization scheme	デフォルトの認可スキーム
Default accounting scheme	デフォルトのチャージ・スキーム
Login authentication scheme	Loginユーザ認証スキーム
Login authorization scheme	Loginユーザ認可スキーム
Login accounting scheme	Loginユーザ課金プラン
Super authentication scheme	ユーザの役割による認証スキームの切り替え
Command authorization scheme	コマンドライン認可スキーム
Command accounting scheme	コマンドライン請求スキーム
Portal authentication scheme	Portalユーザ認証スキーム
Portal authorization scheme	Portalユーザ認可スキーム
Portal accounting scheme	Portalユーザ課金プラン
IKE authentication scheme	IKE拡張認証スキーム
IKE authorization scheme	IKE拡張認証の認可スキーム
IPoE authentication scheme	IPoEユーザ認証スキーム
IPoE authorization scheme	IPoEユーザ認可スキーム
IPoE accounting scheme	IPoEユーザ課金プラン
RADIUS	RADIUSシナリオ
HWTACACS	HWTACACSシナリオ
LDAP	LDAPスキーマ
Local	ローカル・スキーマ
None	無認証、無許可、無課金

フィールド	説明
Accounting start failure action	ユーザの課金開始に失敗したアクション。次の値があります。 • Online:ユーザの請求が失敗した場合、ユーザをオンラインのままにしておく • Offline:ユーザの課金開始に失敗した場合、ユーザを強制的にオフラインにする
Accounting update failure max-times	ユーザが更新の失敗を連続して請求できる回数
Accounting update failure action	ユーザの請求更新に失敗したアクション。次の値が含まれます。 • Online:ユーザ課金の更新に失敗した場合、ユーザをオンラインのままにする • Offline:ユーザ課金の更新に失敗した場合、ユーザを強制的にオフラインにする
Accounting quota out policy	ユーザ課金クォータ枯渇ポリシーには、次の値が含まれます。 • Online:ユーザ課金クォータが使い果たされた場合、ユーザをオンラインのままにしておく • Offline:ユーザ課金クォータが使い果たされた場合、ユーザを強制的にオフラインにする • Redirect:リダイレクト URL の送信
Redirect URL	強制リダイレクトURL
Stop accounting	課金サーバへの課金停止メッセージの送信
User profile	ユーザに送信されるUser Profileの名前
Send accounting update	ユーザークォータが枯渇した後、新しいクォータを取得するための課金更新メッセージを送信するかどうか: • Yes:送信 • No:送信しません
ITA service policy	ITAビジネス戦略の採用
Service type	ISPドメインのビジネスタイプ。HSI、STB、およびVoIPの値を取ります。

フィールド	説明
Session time	ユーザが異常にオフラインになったときに、アプライアンスがサーバにアップロードされたユーザのオンライン時間: • Include idle time:ユーザのアイドル状態の切断時間を保持する • Exclude idle time:ユーザー・アイドル・シャットダウン時間の控除
User address type	ユーザーアドレスタイプ
User basic service IP type	ホスト・アドレス • IPv4:IPv4 アドレスタイプ • IPv6:IPv6 アドレスタイプ • IPv6-PD:IPv6 PD プレフィックス
DHCPv6-follow-IPv6CP timeout	(未サポート) PPPoE/L2TPユーザがIPv6アドレス/PDの割り当てを待機する最大時間(単位は秒です) 設定されていない場合は、Not configuredと表示されます。
Dual-stack accounting method	デュアルスタックユーザの請求方法。次の値が含まれます。 • Merge:ユニファイドアカウンティング、つまりデュアルプロトコルスタックユーザの IPv4 トラフィックと IPv6 トラフィックをまとめて課金サーバにアップロードする • Separate:デュアルプロトコルスタックユーザの IPv4 トラフィックと IPv6 トラフィックを別々に課金サーバにアップロードする
NAS-ID	デバイスのNAS-ID 構成されていない場合は、N/Aと表示されます。
Web server URL	ウェブサーバのURL
Web server URL parameters	ウェブサーバのURL
Web server IPv4 address	IPv4アドレス
Web server IPv6 address	WebサーバのIPv6アドレス
Authorization attributes	ISPのユーザ認証プロパティ

フィールド	説明
Idle cut	ユーザ・アイドル・シャットダウン機能には、次の値があります。 • Enabled:オンになっていると、ISP ドメインのユーザが指定された最大アイドルストップ時間内に生成したトラフィックが、指定された最小データトラフィックを下回ると、強制的にオフラインになります。 • Disabled:ユーザがアイドル状態の切断制御を行わないことを示すクローズ状態。これがデフォルトです。
Idle timeout	ユーザアイドル切断時間(単位は分です)
Flow	ユーザデータトラフィックのしきい値(単位はバイトです)
Traffic direction	次の値を含む、ユーザデータトラフィックの統計方向。 • Both:ユーザの双方向データトラフィックを表します。 • Inbound:ユーザのアップストリームデータトラフィックを表します。 • Outbound:ユーザのダウンストリームデータトラフィックを表します。
IP pool	許可されたIPv4アドレスプールの名前
User profile	権限User Profileの名前
Session group profile	権限Session Group Profileの名前
Inbound CAR	許可された入力方向CAR (CIR:ビット/秒単位の認定情報レート;PIR:ビット/秒単位のピーク情報レート)。入力方向CARが許可されていない場合は、N/Aと表示されます。
Outbound CAR	認可のアウトバウンドCAR (CIR:ビット/秒単位の認定情報レート;PIR:ビット/秒単位のピーク情報レート)。CARへの出力が許可されていない場合は、N/Aと表示されます。
ACL number	許可ACL番号
User group	権限User groupの名前
IPv6 prefix	IPv6プレフィックスの許可
IPv6 pool	許可されたIPv6アドレスプールの名前
Primary DNS server	プライマリDNSサーバのIPv4アドレスの承認
Secondary DNS server	DNSサーバのIPv4アドレスからの認証
Primary DNSV6 server	プライマリDNSサーバのIPv6アドレスの承認
Secondary DNSV6 server	DNSサーバのIPv6アドレスからの認証
URL	リダイレクトURLの承認
IGMP access limit	許可されたIPv4ユーザが同時にリクエストできる最大プログラム数
MLD access limit	許可されたIPv6ユーザが同時にリクエストできる最大プログラム数
Inbound user priority	アップストリームのユーザ優先度を許可

フィールド	説明
Outbound user priority	ダウンストリームユーザー優先順位の付与
User session timeout	認証ユーザセッションのタイムアウト時間 (秒)
Default domain name	デフォルトのISPドメイン名

3.1.13 domain

Syntax

形式 1:

domain name *isp-name*

undo domain name *isp-name*

形式 2:

domain *isp-name*

undo domain *isp-name*

デフォルト

system という ISP ドメインが存在します。

View

System view

定義済みユーザロール

network-admin

パラメータ

name isp-name:ISP ドメイン名。1~255 文字の文字列。大文字と小文字は区別されません。「/」 、「¥」 、「|」 、「」、「:」 、「*」 、「?」 、「<」 、「>」 、「@」の文字を入力します。name パラメータを指定しないコマンドライン形式の場合、ISP ドメイン名は 1~255 文字の文字列で、大文字と小文字は区別されません。「/」 、「¥」 、「|」 、「」、「:」 、「*」 、「?」 、「<」 、「>」 及び「@」 の文字であって、文字列 「d」 、「de」、「def」、「デファ」、「defau」、「defaul」、「default」、「i」 、「if」、「if-」、「」、「if-un」、「if-unk」、「if-unkn」、「if-unkno」、「if-unknow」及び「if-unknown」であってはならない。

説明

domain コマンドを使用して ISP ドメインを作成し、ISP domain view に移動します。指定した ISP ドメインがすでに存在する場合は、ISP domain view に直接移動します。

undo domain コマンドを使用して、指定した ISP ドメインを削除します。

作成されたすべての ISP ドメインは、active の状態になります。

システムで事前定義された ISP ドメイン system は削除できません。変更できるのは、そのドメインの構成だけです。

システムのデフォルト ISP ドメインである ISP ドメインは削除できません。システムのデフォルトの ISP ドメインを削除するには、まず **undo domain default enable** コマンドを使用してデフォルト以外の ISP ドメインに戻します。

アプライアンスに設定されている ISP ドメイン名はできるだけ短くすることをお勧めします。ユーザは、ドメイン名を含むユーザ名をクライアントがサポートできる最大ユーザ名より長く入力しないでください。

例

#test という名前の ISP ドメインを作成し、ビューに移動します。

<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test]

関連コマンド

display domain

domain default enable

domain if-unknown

state (ISP domain view)

3.1.14 domain default enable

Syntax

domain default enable *isp-name*

undo domain default enable

デフォルト

システムのデフォルトの ISP ドメインがあります。名前は system です。

View

System view

定義済みユーザロール

network-admin

パラメータ

isp-name:ISP ドメイン名。1~255 文字の文字列で、大文字と小文字は区別されず、すでに存在している必要があります。

説明

domain default enable コマンドを使用して、ログイン時に ISP ドメイン名を指定しなかったすべてのユーザが属するシステムのデフォルトの ISP ドメインを設定します。

undo domain default enable コマンドを使用して、デフォルトの状態を復元します。

デフォルトの ISP ドメインは 1 つだけシステムに存在できます。

デフォルトとして設定されている ISP ドメインは削除できません。システムのデフォルトの ISP ドメインを削除するには、まず **undo domain default enable** コマンドを使用してデフォルト以外の ISP ドメインに戻します。

例

#新しい ISP ドメイン test を作成し、システムのデフォルトの ISP ドメインに設定します。

<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] quit
[Sysname] domain default enable test

関連コマンド

display domain

domain

3.1.15 local-server log change-password-prompt

Syntax

local-server log change-password-prompt

undo local-server log change-password-prompt

デフォルト

パスワード変更定期アラートログ機能がオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

local-server log change-password-prompt コマンドを使用して、パスワード変更の定期的な警告ログ機能を有効にします。

undo local-server log change-password-prompt コマンドを使用して、パスワード変更の定期的な警告ログ機能をオフにします。

この機能を使用して、Telnet、SSH、HTTP、HTTPS、NETCONF over SSH、および NETCONF over SOAP ユーザのパスワード保護を強化し、システムセキュリティを向上させます。

この機能を使用すると、デバイスでログを生成して、ユーザのログイン時に 24 時間間隔で弱いパスワードを変更するようにユーザに促すことができます。

パスワードは、次の要件を満たさない場合に弱いパスワードとなります。

- **password-control composition** コマンドを使用して設定されるパスワード構成制限。
- **password-control length** コマンドを使用して設定される最小パスワード長制限。
- **password-control complexity** コマンドを使用して設定されるパスワード複雑性チェックポリシー。

NETCONF over SSH または NETCONF over SOAP ユーザーの場合、次のいずれかの条件が存在すると、デバイスはパスワード変更のプロンプトログも生成します。

- ユーザの現在のパスワードがデフォルトのパスワードであるか、有効期限が切れています。
- ユーザは、初めてデバイスにログインするか、グローバルパスワード管理が有効になった後に新しいパスワードを使用してログインします。

次のいずれかの条件が存在する場合、デバイスはユーザーのパスワード変更プロンプトログを生成しなくなります。

- パスワード変更プロンプトログ機能は無効になっています。
- ユーザがパスワードを変更し、新しいパスワードがパスワード管理要件を満たしています。
- 関連するパスワード管理機能の有効化ステータスが変更され、ユーザの現在のパスワードがパスワード管理要件を満たしています。
- パスワード構成ポリシーまたはパスワードの最小長が変更されました。

パスワード管理設定を表示するには、**display password-control** コマンドを使用します。パスワード管理コマンドの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*3 章 パスワード管理*”を参照してください。

例

#パスワード変更の定期的な警告ログ機能を有効にします。

<Sysname> system-view
[Sysname] local-server log change-password-prompt

関連コマンド

display password-control (ユーザアクセスと認証/パスワード管理)

password-control composition (ユーザアクセスと認証/パスワード管理)

password-control length (ユーザアクセスと認証/パスワード管理)

3.1.16 nas-id

Syntax

nas-id *nas-identifier*

undo nas-id

デフォルト

設定なし

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

nas-identifier:NAS-ID (大文字と小文字を区別する 1 から 253 文字の文字列) を指定します。

説明

ISP ドメインの NAS-ID を設定するには、**nas-id** コマンドを使用します。

ISP ドメインから NAS-ID を削除するには、**undo nas-id** コマンドを使用します。

RADIUS 認証中、デバイスは NAS-ID を使用して RADIUS パケットの NAS-Identifier 属性を設定し、RADIUS サーバがユーザのアクセス場所を識別できるようにします。

NAS-ID は、ISP domain view で設定できます。

NAS-ID を選択しない場合、デバイスはデバイス名を NAS-ID として使用します。

例

#ISP ドメインテストをテストする NAS-ID を設定します。

<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] nas-id test

3.1.17 state (ISP domain view)

Syntax

state { **active** | **block** [**time-range**] [**offline**] }

undo state

デフォルト

現在の ISP ドメインがアクティブです。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

active:現在の ISP ドメインがアクティブであることを指定します。つまり、そのドメインの下のユーザがネットワークサービスをリクエストできるようになります。

block:現在の ISP ドメインがブロックされている、つまり、そのドメインのユーザがネットワークサービスを要求できないようにすることを指定します。このパラメータは、公開鍵認証を使用する SSH ユーザを除くすべてのアクセスタイプのユーザに有効です。

time-range:ISP ドメインの期間ベースのブロックを指定します。このパラメータを指定しない場合、ISP ドメインは常にブロックされています。

offline:ISP ドメインがアクティブ状態からブロッキング状態に切り替わると、その ISP ドメインを介してアクセスしているネットワークアクセスクラス(Portal、IPoE を含む)のユーザが強制的にオフラインにされることを示す。このパラメータを指定しない場合、ISP ドメインの状態がブロッキング状態に切り替わっても、現在のユーザの状態には影響しません。

説明

state コマンドは、現在の ISP ドメインの状態を設定します。

undo state コマンドを使用して、デフォルトの状態を復元します。

time-range キーワードを使用して ISP ドメインが期間に基づいてブロックされるように指定すると、ISP ドメインは **state block time-range name** コマンドで指定された期間だけブロックされます。

例

#現在の ISP ドメイン test がブロックされていることを設定します。

```
<Sysname> system-view
[Sysname] domain name test
[Sysname-isp-test] state block
```

関連コマンド

display domain

state block time-range name

3.2 ローカルユーザ構成コマンド

3.2.1 access-limit

Syntax

access-limit *max-user-number*

undo access-limit

デフォルト

現在のローカルユーザ名を使用してアクセスするユーザの数は制限されません。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

max-user-number:現在のローカルユーザ名を使用してデバイスにアクセスするユーザの最大数を示します。範囲は 1~1024 です。

説明

access-limit コマンドは、現在のローカルユーザ名を使用してデバイスにアクセスする最大ユーザ数を設定します。

undo access-limit コマンドを使用して、デフォルトの状態を復元します。

ネットワークアクセスクラスのローカルユーザの場合、ユーザがアクセスする ISP domain view で **accounting start-fail offline** コマンドを設定する必要もあります。そうしないと、現在のユーザ名を使用してアクセスするユーザの数は **access-limit** コマンドによって制限されません。

FTP/SFTP/SCP ユーザは課金をサポートしていないため、FTP/SFTP/SCP ユーザはこの属性の制限を受けません。

例

#ローカルユーザ名 abc で同時にオンラインにできるユーザの数は 5 です。

<Sysname> system-view
[Sysname] local-user abc
[Sysname-luser-manage-abc] access-limit 5

関連コマンド

accounting start-fail offline

display local-user

3.2.2 authorization-attribute (Local user view/user group view)

Syntax

authorization-attribute { **acl** *acl-number* | **idle-cut** *minutes* | **ip** *ipv4-address* | **ip-pool** *ipv4-pool-name* | { **primary-dns** | **secondary-dns** } { **ip** *ipv4-address* } | **session-group-profile** *session-group-profile-name* | **session-timeout** *minutes* | **subscriber-id** *subscriber-id* | **user-profile** *profile-name* | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } *

undo authorization-attribute { **acl** | **idle-cut** | **ip** | **ip-pool** | **primary-dns** | **secondary-dns** | **session-group-profile** | **session-timeout** | **subscriber-id** | **user-profile** | **user-role** *role-name* | **vlan** | **work-directory** } *

デフォルト

許可 FTP/SFTP/SCP ユーザがアクセスできるディレクトリはデバイスのルートですが、アクセス権はありません。

ユーザロール network-admin または level-15 のユーザによって作成されたローカルユーザは、ユーザロール network-operator を付与されます。

View

Local user view

User group view

定義済みユーザロール

network-admin

パラメータ

acl *acl-number*:ローカルユーザの許可 ACL を指定します。ここで、acl-number は認可 ACL の番号で、値の範囲は 2000~5999 です。許可 ACL ルールに一致するトラフィックは、ルールで指定された permit または deny アクションに従って処理されます。

idle-cut *minutes*:ローカルユーザのアイドル状態の切断時間を設定します。ここで、minutes は設定されたアイドル切断時間であり、 1~120 の範囲の値をとり、単位は分である。ユーザがオンラインになってからアイドル状態が続く時間がこの値を超えると、デバイスはそのユーザを強制的にオフラインにします。

ip *ipv4-address*:ローカルユーザの固定 IP アドレスを指定します。ローカルユーザ認証が成功すると、その IP アドレスの使用が許可されます。

ip-pool *ipv4-pool-name*:ローカルユーザの IPv4 アドレスプール情報を指定します。ローカルユーザ認証が成功すると、IPv4 アドレスプールを使用してアドレスを割り当てることができます。ここで、ipv4-pool-name はアドレスプール名を表し、1~63 文字の文字列です。大文字と小文字は区別されません。

primary-dns ip *ipv4-address*:ローカルユーザのプライマリ DNS サーバ IPv4 アドレスを指定します。ローカルユーザ認証が成功すると、プライマリ DNS サーバの使用が許可されます。

secondary-dns ip *ipv4-address*:DNS サーバからのローカルユーザの IPv4 アドレスを指定します。ローカルユーザ認証が成功すると、そのスレーブ DNS サーバの使用が許可されます。

session-group-profile *session-group-profile-name*:ローカルユーザの許可を指定します。本パラメータは現在サポートしていません。

session-timeout *minutes*:ローカルユーザのセッションタイムアウト時間を設定します。ここで、minutes はセッションタイムアウトに設定された時間で、1~1440 の範囲内の値を分単位で指定します。ユーザのオンライン時間がこの値を超えると、デバイスはそのユーザを強制的にオフラインにします。

subscriber-id *subscriber-id*:ローカルユーザ認可 Subscriber ID を 1~4095 の値の範囲で設定します。本パラメータは現在サポートしていません。

user-profile *profile-name*:ローカルユーザの許可を指定します。本パラメータは現在サポートしていません。

user-role *role-name*: 権限のあるユーザロールを指定します。role-name 引数は、1 から 63 文字の大文字と小文字を区別する文字列です。ユーザには最大 64 個のユーザロールを指定できます。ユーザロール関連のコマンドについては、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。このオプションは Local user view でのみ使用でき、User group view では使用できません。

vlan vlan-id:ローカルユーザの許可 VLAN を指定します。ここで、vlan-id は VLAN 番号で、範囲は 1~4094 です。ローカルユーザ認証が成功すると、指定された VLAN 内のネットワークリソースのみにアクセスすることが許可されます。

wlan-vlan *wlan-vlan-id*:無線ユーザが属する VLAN を示す。ここで、wlan-vlan-id は VLAN ID、値の範囲は 1~4094 です。この属性は、ワイヤレスアクセスユーザにのみ有効です。

wlan-vlan-group *wlan-vlan-group-name*:無線ユーザが属する VLAN グループを示す。ここで、wlan-vlan-group-name は VLAN グループの名前、1~32 文字の文字列、大文字と小文字が区別され、先頭の文字は英字である必要があります。この属性は、ワイヤレスアクセスユーザにのみ有効です。

work-directory *directory-name*:FTP/SFTP/SCP ユーザがアクセスできるディレクトリを許可します。ここで、directory-name は、FTP/SFTP/SCP ユーザがアクセスできるディレクトリを表します。ディレクトリは 1~255 文字の文字列で、大文字と小文字は区別されません。ディレクトリはすでに存在している必要があります。

説明

authorization-attribute コマンドは、ローカルユーザまたはユーザグループの認証属性を設定します。この属性は、ローカルユーザの認証が完了した後に、デバイスからユーザに送信されます。

undo authorization-attribute コマンドは、指定された認証属性を削除し、ユーザが持つデフォルトのアクセス権を復元します。

構成可能な認可属性には、使用環境と目的が明確に設定されています。ユーザのサービスタイプに対応する認可属性を構成します。

IPoE ユーザの場合、許可属性 idle-cut、ip-pool、primary-dns、secondary-dns、session-group-profile、session-timeout、subscriber-id、user-profile のみが有効です。

Portal ユーザの場合、許可属性 ip-pool、session-timeout、user-profile、acl のみが有効です。

Telnet、Terminal、SSH ユーザの場合、認証属性 idle-cut、user-role のみが有効です。

http、https ユーザの場合、許可属性 user-role のみが有効です。

FTP ユーザの場合、許可属性 user-role、work-directory のみが有効です。

IKE ユーザの場合、認証属性 ip-pool のみが有効です。

他のタイプのローカルユーザでは、すべての認証属性が無効です。

ユーザグループの認可属性は、グループ内のすべてのローカルユーザに対して有効であるため、同じ属性を持つユーザは、同じユーザグループに参加することで、構成と管理を統一できます。

Local user view で構成されていない認可属性は、所属するユーザグループの認可属性構成を継承しますが、Local user view と所属する User group view の両方で認可属性が構成されている場合は、Local user view の認可属性が有効になります。

ローカルユーザがこのコマンドで指定された承認されたユーザロールのみを使用するようにするには、まず undo authorization-attribute user-role コマンドを使用して、そのユーザがすでに持っているデフォルトのユーザロールを削除します。

セキュリティログ管理者の権限を持つローカルユーザは、デバイスにログインすると、セキュリティログファイルの管理に関連するコマンドと、セキュリティログファイルの操作に関連するコマンドのみを実行できます。これらのコマンドは、display role name security-audit コマンドで表示できます。セキュリティログファイルの管理に関連するコマンドについては、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*3 システム管理*”の”*5 章 Information Center*”を参照してください。ファイルシステム管理関連のコマンドについては、QX-W2300AC シリーズアクセスコントローラコマンドマニュアルの“*2 基本機能*”の”*6 章 ファイルシステム管理*”を参照してください。

ローカルユーザにセキュリティログ管理者の役割を付与する場合は、次の点に注意してください。

セキュリティログ管理者ロールとその他のユーザロールは相互に排他的です。

- 1 人のユーザにセキュリティログ管理者の役割を付与する場合、現在のユーザの他のすべてのユーザの役割を削除するかどうかを確認するプロンプトが表示されます。
- 現在のユーザのセキュリティログ管理者の役割がすでに承認されており、別のユーザの役割が承認されると、現在のユーザのセキュリティログ管理者の役割を削除するかどうかを確認するメッセージが表示されます。

システムの最後のセキュリティログ管理者ロールのローカルユーザは削除できません。

例

#ネットワークアクセスクラスを設定して下さい。ローカルユーザ abc のための許可 VLAN は VLAN 2 です。

<Sysname> system-view
[Sysname] local-user abc class network
[Sysname-luser-network-abc] authorization-attribute vlan 2

#ユーザグループ abc のための許可 VLAN を VLAN 3 に設定して下さい。

<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc] authorization-attribute vlan 3

#デバイス管理クラスの設定ローカルユーザ xyz の許可されたユーザの役割は security-audit です(セキュリティログ管理者)。

<Sysname> system-view
[Sysname] local-user xyz class manage
[Sysname-luser-manage-xyz] authorization-attribute user-role security-audit
This operation will delete all other roles of the user.Are you sure?[Y/N]:y

関連コマンド

display local-user

display user-group

3.2.3 bind-attribute

Syntax

bind-attribute { **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } *

undo bind-attribute { **call-number** | **ip** | **location** | **mac** | **vlan** } *

デフォルト

ユーザのバインドプロパティが設定されていません。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

location *interface interface-type interface-number*:ユーザがバインドするインタフェースを指定します。ここで、interface-type interface-number はインターフェイスタイプとインタフェース番号を表します。ユーザがアクセスするインタフェースが、ここでバインドされているインタフェースと一致しない場合、認証は失敗します。このバインド属性は、IPoE タイプ Portal のユーザのみに適用されます。

mac *mac-address*:ユーザの MAC アドレスを指定します。ここで、mac-address は H-H-H 形式です。このバインド属性は、IPoE タイプ Portal のユーザのみに適用されます。

vlan *vlan-id*:ユーザが属する VLAN を指定します。ここで、vlan-id は VLAN 番号で、範囲は 1~4094 です。このバインド属性は、IPoE タイプ Portal のユーザのみに適用されます。

説明

bind-attribute コマンドは、ユーザのバインドプロパティを設定します。

undo bind-attribute コマンドは、指定されたユーザーバインドプロパティーを削除します。

デバイスがユーザをローカルに認証すると、ユーザの実際の属性が構成済みのバインド属性と一致するかどうかがチェックされます。一致しない場合、またはユーザがバインド属性を持っていない場合、認証は失敗します。

バインドプロパティの検出では、ユーザのアクセスサービスタイプは区別されないため、バインドプロパティを設定する際には、特定のアクセスタイプのユーザが特定のプロパティをバインドする必要があるかどうかが考慮されます。

インタフェースのプロパティをバインドするときは、インタフェースの型が適切かどうかを考慮します。Portal ユーザの場合、Portal を有効にするインタフェースが VLAN インタフェースで、**portal roaming enable** コマンドで Portal ユーザローミング機能が設定されていない場合、ユーザが実際にアクセスするレイヤ 2 イーサネットインターフェイスとしてバインドされたインタフェースを設定します。その他の場合、バインドを構成するインタフェースは、Portal を有効にするインタフェースです。

例

#ネットワークアクセスクラスの設定ローカルユーザ abc のバインド MAC アドレスは 11-11-11 です。

```
<Sysname> system-view
[Sysname] local-user abc class network
[Sysname-luser-network-abc] bind-attribute mac 11-11-11
```

関連コマンド

display local-user

3.2.4 description

Syntax

description *text*

undo description

デフォルト

ネットワークアクセスクラスのローカルユーザの説明情報が設定されていません。

View

ネットワークアクセスクラスの Local user view

定義済みユーザロール

network-admin

パラメータ

text:ユーザの説明情報。1~255 文字の文字列で、大文字と小文字が区別されます。

説明

description コマンドは、ネットワークアクセスクラスのローカルユーザのプロファイル情報を設定します。

undo description コマンドを使用して、デフォルトの状態を復元します。

ローカルユーザの説明情報が#user_from_server#という固定文字列に設定されている場合は、そのユーザが特定の目的のために表示および管理に使用できるように特別に識別されていることを意味します。具体的な目的は、管理側の実装に準じてください。

例

#設定ネットワークアクセスクラスローカルユーザ 123 のための記述情報は Manager of MSC company です。

<Sysname> system-view
[Sysname] local-user 123 class network
[Sysname-luser-network-123] description Manager of MSC company

関連コマンド

display local-user

3.2.5 display local-user

Syntax

display local-user [**class** { **manage** | **network** [**guest**] } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **http** | **https** | **ike** | **ipoe** | **portal** | **ssh** | **telnet** | **terminal** } | **state**

{ **active** | **block** } | **user-name** *user-name* **class** { **manage** | **network** [**guest**] } | **vlan** *vlan-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

class:指定したユーザカテゴリのローカルユーザ情報を表示します。

manage:デバイス管理クラスのユーザ。

network:ネットワークアクセスクラスユーザ。

guest:ゲストユーザ。

idle-cut {disable |enable }:アイドル・カット機能のオン/オフを切り替えるローカルユーザ情報を表示します。ここで、disable は、アイドル・カット機能が有効になっていないローカルユーザを示します。enable は、アイドル・カット機能が有効で、アイドル・カット時間が設定されているローカルユーザを示します。

service-type:指定したユーザタイプのローカルユーザ情報を表示します。

ftp:FTP ユーザ。

http:HTTP ユーザ。

https:HTTPS ユーザ。

ike:IKE 拡張認証ユーザ。

ipoe:IPoE ユーザー(主に IP 接続ユーザー、例えば 2/3 層専用線ユーザー、デジタルセットトップボックス接続ユーザーを指す。)。

portal:Portal ユーザ。

ssh:SSH ユーザ。

telnet:Telnet ユーザ。

termi*nal*:Console からログインしたエンドユーザ。

state {active |block }:指定した状態のローカルユーザ情報を表示します。ここで、active はユーザがアクティブであることを示します。つまり、ユーザがネットワークサービスを要求できるようになります。block は、ユーザがブロックされていることを示します。つまり、システムはユーザにネットワークサービスを要求できません。

*user-name user-nam*e:指定したユーザ名のローカルユーザ情報を表示します。ここで、user-name はローカルユーザ名を表します。1~80 文字の文字列で、「プレーンユーザー名@ドメイン名」または純粋なユーザ名を使用できます。純粋なユーザ名では大文字と小文字が区別され、記号 「¥」 、 「|」 、 「/」 、 「:」 、 「*」 、 「?」 は使用

できません。」 、 「<」 、 「>、 「@」 、 「a」 、「al」、「all」は使用できません。ドメイン名では大文字と小文字は区別されず、 「@」 記号は使用できません。

vlan vlan-id:指定した VLAN 内のすべてのローカルユーザ情報を表示します。ここで、vlan-id は VLAN 番号で、範囲は 1~4094 です。

説明

display local-user コマンドを使用して、ローカルユーザの構成情報とオンラインユーザ数の統計情報を表示します。

パラメータを指定しない場合は、すべてのローカルユーザ情報が表示されます。

例

#すべてのローカルユーザに関する情報を表示します。

<Sysname> display local-user

Total 1 local users matched.

Device management user root:
State: Active
Service type: SSH/Telnet/Terminal
Access limit: Enabled
Max access number: 3
Current access number: 1
User group: system
Bind attributes:
Authorization attributes:
Work directory: flash:
User role list: network-admin
Password control configurations:
Password aging: 3 days
Password history was last reset: 0 days ago
Password remaining lifetime: 2 days 12 hours 30 minutes 30 seconds

表 3-2 display local-user コマンドの表示情報の説明

フィールド	説明
Total x local users matched.	合計xのローカルユーザー一致
State	ローカルユーザ状態 • Active:アクティブステータス • Block:ブロック状態
Service type	ローカルユーザが使用するサービスタイプ

フィールド	説明
Access limit	そのユーザ名を使用するアクセスユーザ数を制限するかどうか
Max access number	最大アクセスユーザ数
Current access number	ユーザ名を使用する現在のアクセスユーザ数
User group	ローカルユーザが属するユーザグループ
Bind attributes	ローカルユーザのバインド属性
IP address	ローカルユーザのIPアドレス
Location bound	ローカルユーザがバインドするポート
MAC address	ローカルユーザのMACアドレス
VLAN ID	ローカルユーザがバインドしたVLAN
WLAN VLAN ID	ローカルワイヤレスユーザ許可VLAN
WLAN VLAN group name	ローカルワイヤレスユーザ認可VLANグループ
Authorization attributes	ローカルユーザの認可属性
Idle timeout	ローカルユーザのアイドル切断時間(単位は分です)
Session-timeout	ローカルユーザのセッションのタイムアウト(単位は分です)
Work directory	FTP/SFTP/SCPユーザがアクセスできるディレクトリ
ACL number	ローカルユーザ許可ACL
VLAN ID	ローカルユーザ認可VLAN
User profile	ローカルユーザ認可User Profile
User role list	ローカルユーザの認可ユーザの役割リスト
IP pool	ローカルユーザの許可されたIPv4アドレスプール
IP address	ローカルユーザの認証IPv4アドレス
IPv6 address	ローカルユーザの認証IPv6アドレス
IPv6 prefix	ローカルユーザの認証IPv6プレフィックス
IPv6 pool	ローカルユーザの許可されたIPv6アドレスプール
Primary DNS server	ローカルユーザの認証プライマリDNSサーバのIPv4アドレス
Secondary DNS server	ローカルユーザの許可DNSサーバからのIPv4アドレス
Primary DNSV6 server	ローカルユーザの許可プライマリDNSサーバIPv6アドレス
Secondary DNSV6 server	DNSサーバIPv6アドレスからのローカルユーザの許可
Subscriber ID	ローカルユーザの許可Subscriber ID
Session group profile	ローカルユーザの許可Session Group Profile
Password control configurations	ローカルユーザのパスワード管理プロパティ
Password aging	パスワードエージング時間
Password length	パスワードの最小長
Password composition	パスワードの組み合わせポリシー(パスワード要素の組み合わせのタイプ、少なくとも各要素の数)

フィールド	説明
Password complexity	パスワードの複雑度チェックポリシー(ユーザ名が含まれているかどうか、またはユーザ名が逆になっているかどうか;同じ文字が3つ以上含まれているかどうか)
Maximum login attempts	ユーザの最大ログイン試行回数
Action for exceeding login attempts	ログイン試行回数が設定回数に達した後のユーザアカウントのロック動作
Password history was last reset	パスワード履歴が最後にクリアされた時刻
Password remaining lifetime	残りのパスワードエージング時間
Full name	ローカルゲストユーザの名前
Company	ローカルゲストユーザの会社
Email	ローカルゲストユーザのEmailアドレス
Phone	ローカルゲストユーザの電話番号
Sponsor full name	ローカルゲストユーザ受付者の名前
Sponsor department	ローカルゲストユーザ・コンシェルジュの所属部門
Sponsor email	ローカルのゲストユーザコンシェルジュのEmailアドレス
Description	ネットワークアクセスクラスのローカルユーザの記述情報
Validity period	ネットワークアクセスクラスローカルユーザ有効期間
Start date and time	ネットワークアクセスクラスのローカルユーザが有効になり始めた日時
Expiration date and time	ネットワークアクセスクラスのローカルユーザの有効期限と時刻

3.2.6 display user-group

Syntax

display user-group { **all** | **name** *group-name* } [**identity-member** { **all** | **group** | **user** }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all:すべてのユーザグループの構成情報を表示します。

name group-name:指定したユーザグループの構成を表示します。group-name はユーザグループ名で、1~32 文字の文字列です。大文字と小文字は区別されません。

説明

display user-group コマンドを使用して、ユーザグループの構成情報を表示します。

例

#すべてのユーザグループに関連する構成を表示します。

<Sysname> display user-group all

Total 2 user groups matched.

User group: system
  Authorization attributes:
    Work directory: flash:
User group: jj
  Authorization attributes:
    Idle timeout: 2 minutes
    Work directory: flash:/
    ACL number: 2000
    VLAN ID: 2
    User profile: pp
  Password control configurations:
    Password aging: 2 days

表 3-3 display user-group コマンドの表示情報の説明

フィールド	説明
Total 2 user groups matched.	合計2つのユーザグループが一致しました
User group	ユーザグループ名
Authorization attributes	認可属性情報
Idle timeout	アイドル切断時間(単位:分)
Session-timeout	セッションのタイムアウト時間(単位:分)
Work directory	FTP/SFTP/SCPユーザがアクセスできるディレクトリ
ACL number	許可ACL番号
VLAN ID	許可VLAN ID
User profile	認可User Profile名
IP pool	IPv4アドレスプールの承認
IPv6 prefix	IPv6プレフィックスの許可
IPv6 pool	IPv6アドレスプールの承認
Primary DNS server	プライマリDNSサーバのIPv4アドレスの承認
Secondary DNS server	DNSサーバのIPv4アドレスからの認証
Primary DNSV6 server	プライマリDNSサーバのIPv6アドレスの承認
Secondary DNSV6 server	DNSサーバのIPv6アドレスからの認証
Password control configurations	ユーザグループのパスワード管理プロパティ

フィールド	説明
Password aging	パスワードエージング時間
Password length	パスワードの最小長
Password composition	パスワードの組み合わせポリシー(パスワード要素の組み合わせのタイプ、少なくとも各要素の数)
Password complexity	パスワードの複雑度チェックポリシー(ユーザ名が含まれているかどうか、またはユーザ名が逆になっているかどうか;同じ文字が3つ以上含まれているかどうか)
Maximum login attempts	ユーザの最大ログイン試行回数
Action for exceeding login attempts	ログイン試行回数が設定回数に達した後のユーザアカウントのロック動作
Identity users	ユーザタイプのアイデンティティー・メンバーの数
Identity groups	ユーザー・グループ・タイプのアイデンティティー・メンバーの数
User ID	ユーザのID
Group ID	ユーザグループのID
Username	ユーザの名前
Group name	ユーザグループの名前

3.2.7 group

Syntax

group *group-name*

undo group

デフォルト

ローカルユーザはユーザグループ system に属しています。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

group-name:ユーザグループ名。1~32 文字の文字列で、大文字と小文字は区別されません。

説明

group コマンドは、ローカルユーザが属するユーザグループを設定します。

undo group コマンドを使用して、デフォルトの構成を復元します。

例

#デバイス管理クラスのローカルユーザ 111 が属するユーザグループを abc に設定する。

<Sysname> system-view
[Sysname] local-user 111 class manage
[Sysname-luser-manage-111] group abc

関連コマンド

display local-user

3.2.8 local-user

Syntax

local-user *user-name* [**class** { **manage** | **network** [**guest**] }]

undo local-user { *user-name* **class** { **manage** | **network** [**guest**] } | **all** [**class** { **manage** | **network** [**guest**] } |**service-type** { **ftp** | **http** | **https** | **ike** | **ipoe** | **portal** | **ssh** | **telnet** | **terminal** }] }

デフォルト

ローカルユーザが存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

user-name:ローカルユーザ名を示す 1~80 文字の文字列。「プレーンユーザー名@ドメイン名」または純粋なユーザ名を指定できます。純粋なユーザ名では大文字と小文字が区別され、記号 「¥」 、 「|」 、 「/」 、 「:」 、 「*」 、 「?」 は使用できません。」 、 「<」 、 「>」 及び 「@」 は、「all」又は「auto-delete」の最初の文字 「a」 から右にいくつかの連続する文字と全く同じ文字列であってはならず、例えば、 「a」 、「al」、「all」、「au」、「aut」、「auto」、「auto-」、「auto-d」等であってはならない。ドメイン名では大文字と小文字は区別されず、 「@」 記号は使用できません。

class:ローカルユーザのカテゴリを指定します。このパラメータを指定しない場合は、デバイス管理クラスのユーザを表します。

manage:デバイスにログインし、デバイスの設定と監視を行うデバイス管理クラスのユーザ。このタイプのユーザは、ftp、http、https、telnet、ssh、terminal サービスを提供できます。

network:デバイスを介してネットワークにアクセスし、ネットワークリソースにアクセスするためのネットワークアクセスクラスのユーザ。このようなユーザは、ike、ipoe、portal サービスを提供できます。

guest:アカウントの有効期間中のみ portal サービスを提供できるゲストユーザ。

all:すべてのユーザ。

service-type:ユーザのタイプを指定します。

ftp:FTP タイプユーザを表す。

http:HTTP タイプのユーザを表します。

https:HTTPS タイプのユーザを示します。

ike:IKE 拡張認証タイプユーザを表します。

ipoe:IPoE タイプのユーザ(主に IP でアクセスするユーザ、例えば 2、3 層の専用線、デジタルセットトップボックスでアクセスするユーザを指す。)を表します。

portal:Portal ユーザを表します。

ssh:SSH ユーザを示します。

telnet:Telnet ユーザを表します。

terminal:Console 口からログインしたエンドユーザを示す。

説明

local-user コマンドを使用して、ローカルユーザを追加し、Local user view に移動します。指定したローカルユーザがすでに存在する場合は、ローカルユーザ表示に直接進みます。

undo local-user コマンドは、指定されたローカルユーザを削除します。

例

#user1 という名前のデバイス管理クラスのローカルユーザを追加します。

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1]
```

#user2 という名前のネットワークアクセスクラスのローカルユーザを追加します。

```
<Sysname> system-view
[Sysname] local-user user2 class network
[Sysname-luser-network-user2]
```

#user3 という名前のネットワークアクセスクラスのローカルゲストユーザを追加します。

```
<Sysname> system-view
[Sysname] local-user user3 class network guest
[Sysname-luser-network (guest)-user3]
```

関連コマンド

display local-user

service-type (Local user view)

3.2.9 password (Device management user view)

Syntax

password [{ **hash** | **simple** } *string*]

undo password

デフォルト

ローカルユーザパスワードが存在しない場合、ユーザ名が有効で他の属性が認証されていれば、ローカルユーザはパスワードを入力せずに認証されます。

View

デバイス管理クラスのローカルユーザ表示

定義済みユーザロール

network-admin

パラメータ

hash:パスワードがハッシュで設定されていることを示します。

simple:パスワードがクリアテキストで設定され、ハッシュされて保存されることを示します。

string:大文字と小文字を区別するパスワード文字列。平文パスワードが 1~63 文字の文字列;ハッシュパスワード 1~110 文字の文字列。特殊文字とは 「?」 以外のすべての表示文字(表示文字の ASCII コード区間は 32~126 です。)。必要に応じて、"」 、 「¥」 の場合は、エスケープ文字「¥」 を使用して入力する必要があります。つまり、実際には「¥」を入力する必要があります。"、「¥¥¥」の文字を含めます。スペースを入力する場合は、文字列全体を二重引用符で囲みます。

説明

password コマンドは、ローカルユーザのパスワードを設定します。

undo password コマンドを使用して、デフォルトの状態を復元します。

パラメータを指定しない場合、パスワードはクリアテキストでインタラクティブに設定されます。

ローカルユーザのパスワードは設定できません。ローカルユーザにパスワードが設定されていない場合は、ユーザ名が有効で他の属性が認証されていれば、ユーザの認証にパスワードを入力する必要はありません。ユーザアカウントのセキュリティを強化するには、ローカルユーザパスワードを設定することをお勧めします。

グローバル Password Control 機能がオンの場合は、次の点に注意してください。

すべての履歴パスワードはハッシュされて保存されます。

現在ログインしているユーザが自分のパスワードを平文で変更する場合は、まず既存の平文パスワードを入力し、次に入力した新しいパスワードがすべての履歴パスワードと異なることを確認します。また、既存のパスワードとは少なくとも 4 文字の違いが必要です。

現在ログインしているユーザが他のユーザのパスワードをクリアテキストで変更する場合は、新しいパスワードがすべての履歴パスワードと異なることを確認する必要があります。

現在ログインしているユーザが自分のパスワードを削除する場合は、既存の平文パスワードが必要です。

その他の場合は、既存の平文パスワードを指定する必要はなく、履歴パスワードと比較する必要もありません。

例

#デバイス管理クラスのローカルユーザ user1 のパスワードをクリアテキストの 123456TESTplat&!に設定します。

```
<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
```

#デバイス管理クラスのローカルユーザ test のパスワードを対話形式で設定します。

```
<Sysname> system-view
[Sysname] local-user test class manage
[Sysname-luser-manage-test] password
Password:
Confirm:
```

関連コマンド

display local-user

3.2.10 password (Network access user view)

Syntax

password { **cipher** | **simple** } *string*

undo password

デフォルト

ローカルユーザパスワードが存在しない場合、ユーザ名が有効で他の属性が認証されていれば、ローカルユーザはパスワードを入力せずに認証されます。

View

ネットワークアクセスクラスの Local user view

定義済みユーザロール

network-admin

パラメータ

cipher:パスワードが暗号文で設定されていることを示します。

simple:パスワードがクリアテキストで設定され、暗号化されたテキストとして保存されることを示します。

string:大文字と小文字を区別するパスワード文字列。平文パスワードが 1~63 文字の文字列;暗号文パスワードは 1~117 文字の文字列です。

説明

password コマンドは、ローカルユーザのパスワードを設定します。

undo password コマンドを使用して、デフォルトの状態を復元します。

ユーザアカウントのセキュリティを強化するには、ローカルユーザパスワードを設定することをお勧めします。

例

#ネットワークアクセスクラスのローカルユーザ user1 のパスワードをクリアテキスト 123456 TESTuser&!に設定します。

<Sysname> system-view
[Sysname] local-user user1 class network
[Sysname-luser-network-user1] password simple 123456TESTuser&!

関連コマンド

display local-user

3.2.11 service-type (Local user view)

Syntax

service-type { **ftp** | **ike** | **ipoe** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * | **portal** }

undo service-type { **ftp** | **ike** | **ipoe** | { **http** | **https** | **ssh** | **telnet** | **terminal** } * | **portal** }

デフォルト

システムはユーザにサービスを許可しません。つまり、ユーザはサービスを使用できません。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

ftp:ユーザが FTP サービスを利用できることを指定する。FTP サービスを許可する場合は、authorization-attribute work-directory コマンドを使用して許可ディレクトリを設定できます。

http:ユーザが HTTP サービスを使用できるように指定します。

https:ユーザが HTTPS サービスを使用できるように指定します。

ike:ユーザが IKE 拡張認証サービスを使用できるように指定します。

ipoe:ユーザが IPoE サービスを使用できるように指定します。

ssh:ユーザが SSH サービスを使用できるように指定します。

telnet:ユーザが Telnet サービスを使用できるように指定します。

terminal:ユーザが terminal サービス(Console からログインします)を使用できるように指定します。

portal:ユーザが Portal サービスを使用できるように指定します。

説明

service-type コマンドは、ユーザが使用できるサービスの種類を設定します。

undo service-type コマンドは、ユーザが使用できるサービスタイプを削除するために使用します。

このコマンドを複数回実行することで、ユーザが使用できるサービスの種類を設定できます。

例

#デバイス管理クラスのユーザが Telnet サービスと FTP サービスを使用できるように指定します。

<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] service-type telnet
[Sysname-luser-manage-user1] service-type ftp

関連コマンド

display local-user

3.2.12 state (Local user view)

Syntax

state { **active** | **block** }

undo state

デフォルト

ローカルユーザがアクティブです。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

active:現在のローカルユーザがアクティブであること、つまり現在のローカルユーザがネットワークサービスを要求できることを指定します。

block:現在のローカルユーザが「閉塞」状態であること、つまり現在のローカルユーザがネットワークサービスを要求できないことを指定します。

説明

state コマンドは、現在のローカルユーザの状態を設定します。

undo state コマンドを使用して、デフォルトの状態を復元します。

例

#デバイス管理クラスの設定ローカルユーザ user1 は「閉塞」状態です。

<Sysname> system-view
[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] state block

関連コマンド

display local-user

3.2.13 user-group

Syntax

user-group *group-name*

undo user-group *group-name*

デフォルト

system という名前のユーザグループが存在します。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name:ユーザグループ名。1~32 文字の文字列で、大文字と小文字は区別されません。

説明

user-group コマンドを使用して、ユーザグループを作成し、User group view に移動します。指定したユーザグループがすでに存在する場合は、ユーザグループ表示に直接進みます。

undo user-group コマンドは、指定されたユーザグループを削除します。

ユーザグループはローカルユーザの集まりであり、一元管理が必要な一部の属性は、ユーザグループ内で一元的に構成および管理できます。

ローカルユーザを含むユーザグループは削除できません。

システムに存在するデフォルトユーザグループ system は削除できませんが、構成は変更できます。

例

#abc という名前のユーザグループを作成し、そのビューに移動します。

<Sysname> system-view
[Sysname] user-group abc
[Sysname-ugroup-abc]

関連コマンド

display user-group

3.3 RADIUS設定コマンド

3.3.1 accounting-on enable

Syntax

accounting-on enable [**interval** *interval* | **send** *send-times*] *

undo accounting-on enable

デフォルト

accounting-on 機能がオフになっています。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

interval interval:accounting-on メッセージの再送間隔を秒単位で 1~15 の範囲で指定します。デフォルト値は 3 です。

send send-times:accounting-on メッセージの最大送信回数を 1～255 の範囲で指定します。デフォルト値は 50 です。

説明

accounting-on enable コマンドは、accounting-on 機能を有効にするために使用します。

undo accounting-on enable コマンドは、accounting-on 機能をオフにするために使用します。

accounting-on 機能は、デバイス全体が、再起動後に、accounting-on メッセージを送信することによって、シナリオによって使用される RADIUS 課金サーバに通知し、RADIUS サーバに課金を停止するように要求し、デバイスのユーザを強制的にオフラインにすることを可能にする。

accounting-on 機能を有効にした後で、save コマンドを実行して、デバイス全体が次回再起動したときに accounting-on 機能が有効になるようにします。

このコマンドで設定した accounting-on パラメータは、すぐに有効になります。

例

#RADIUS シナリオ radius1 で、accounting-on 機能を有効にし、accounting-on メッセージの再送信間隔を 5 秒、accounting-on メッセージの最大送信回数を 15 回に設定します。

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] accounting-on enable interval 5 send 15

関連コマンド

display radius scheme

3.3.2 data-flow-format (RADIUS scheme view)

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

デフォルト

ストリームの単位はバイト、パケットの単位はパケットである。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

data:ストリームの単位を設定します。

byte:ストリームの単位はバイトである。

giga-byte:データストリームの単位ギガバイト。

kilo-byte:ストリームの単位はキロバイトです。

mega-byte:ストリームの単位はメガバイトです。

packet:パケットの単位を設定します。

giga-packet:パケットの単位はギガパケットです。

kilo-packet:パケットの単位は 1000 パケットである。

mega-packet:パケットの単位はメガパケットである。

one-packet:パケットの単位はパケットである。

説明

data-flow-format コマンドは、RADIUS サーバに送信されるトラフィックとパケットの単位を設定します。

undo data-flow-format コマンドを使用して、デフォルトの状態を復元します。

デバイスで設定された RADIUS サーバに送信されるトラフィック単位とパケット単位は、RADIUS サーバのトラフィック統計単位と一致している必要があります。一致していないと、正しく課金されません。

例

#RADIUS シナリオ radius1 では、RADIUS サーバへのトラフィックの単位をキロバイト、パケットの単位を 1000 パケットに設定します。

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet

関連コマンド

display radius scheme

3.3.3 display radius scheme

Syntax

display radius scheme [*radius-scheme-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

radius-scheme-name:RADIUS スキーマ名。1~32 文字の文字列で、大文字と小文字は区別されません。このパラメータを指定しない場合は、すべての RADIUS スキーマを表します。

説明

display radius scheme コマンドは、RADIUS スキーマの構成情報を表示するために使用します。

例

#すべての RADIUS シナリオの設定情報を表示します。

```
<Sysname> display radius scheme
Total 1 RADIUS schemes

------------------------------------------------------------------
RADIUS scheme name: radius1
  Index : 0
  Primary authentication server:
    Host name: Not configured
    IP    : 2.2.2.2                          Port: 1812
    VPN   : Not configured
    State: Active
    Test profile: 132
      Probe username: test
      Probe interval: 60 minutes
      Probe count    : 5
    Weight: 40
  Primary accounting server:
    Host name: Not configured
    IP    : 1.1.1.1                          Port: 1813
```

```
  VPN  : Not configured
  State: Active
  Weight: 40
Second authentication server:
  Host name: Not configured
  IP   : 3.3.3.3                    Port: 1812
  VPN  : Not configured
  State: Block
  Test profile: Not configured
  Weight: 40
Second accounting server:
  Host name: Not configured
  IP   : 3.3.3.3                    Port: 1813
  VPN  : Not configured
  State: Block (Mandatory)
  Weight: 0
Accounting-On function                    : Enabled
  extended function                       : Disabled
  retransmission times                    : 5
  retransmission interval(seconds)        : 2
Timeout Interval(seconds)                 : 3
Retransmission Times                      : 3
Retransmission Times for Accounting Update : 5
Server Quiet Period(minutes)              : 5
Realtime Accounting Interval(seconds)     : 22
Stop-accounting packets buffering         : Enabled
  Retransmission times                    : 500
NAS IP Address                            : 1.1.1.1
Local NAS IP Address                      : Not configured
Peer NAS IP Address                       : Not configured
Source IP Address                         : 1.1.1.1
VPN                                       : Not configured
Username format                           : with-domain
Data flow unit                            : Megabyte
Packet unit                               : One
Attribute 15 check-mode                   : Strict
Attribute 17 carry old password           : Disabled
Attribute 25                              : CAR
Attribute 30 format                       : hh:hh:hh:hh:hh:hh:SSID
Attribute 30 MAC format                   : hh:hh:hh:hh:hh:hh
Attribute 31 MAC format                   : hh:hh:hh:hh:hh:hh
Remanent-Volume threshold                 : 0
Attribute Remanent-Volume unit            : Mega
```

```
RADIUS server version (vendor ID 2011)      : 1.0
server-load-sharing                         : loading-share
Stop-accounting-packet send-force           : Disabled
Authentication response pending limit       : Not configured
Accounting response pending limit           : Not configured
Username authorization                      : Applied
All-server-block action                     : Attempt the top-priority server
Attribute 218 of vendor ID 25506            : DHCP-Option 61
                                              Format 1 (1-byte Type field)
------------------------------------------------------------------
```

表 3-4 display radius scheme コマンドの表示情報の説明

フィールド	説明
Total 1 RADIUS schemes.	合計1つのRADIUSシナリオ
RADIUS scheme name	RADIUSスキーマの名前
Index	RADIUSスキーマの索引番号
Primary authentication server	プライマリRADIUS認証サーバ
Primary accounting server	プライマリRADIUS課金サーバ
Second authentication server	RADIUS認証サーバから
Second accounting server	RADIUSからの課金サーバ
Host name	RADIUS認証/課金サーバのホスト名 構成されていない場合は、Not configuredと表示されます。
IP	RADIUS認証/課金サーバのIPアドレス 構成されていない場合は、Not configuredと表示されます。
port	RADIUS認証/課金サーバのアクセスポート番号 構成されていない場合は、デフォルト値が表示されます。
State	RADIUS認証/課金サーバの現状 • Active:アクティブ状態 • Block:自動変換のサイレント状態 • Block (Mandatory):手動で設定されたサイレント状態
VPN	(未サポート) RADIUS認証/課金サーバまたはRADIUSシナリオが存在するVPN 構成されていない場合は、Not configuredと表示されます。
Test profile	プローブ・サーバのステータスに使用されるテンプレート名
Probe username	プローブ・サーバのステータスに使用されるユーザ名
Probe interval	サーバのステータスを検出する期間(単位は分です)

フィールド	説明
Probe count	各ラウンドの到達性判断に必要な連続探知回数
Weight	RADIUSサーバの重み
Accounting-On function	accounting-on機能がオンになっている場合
extended function	accounting-on拡張機能がオンになっている場合
retransmission times	accounting-onメッセージの送信試行回数
retransmission interval (seconds)	accounting-onメッセージの再送間隔(単位は秒です)
Timeout Interval (seconds)	RADIUSサーバータイムアウト(単位は秒です)
Retransmission Times	RADIUSメッセージを送信する最大試行回数
Retransmission Times for Accounting Update	リアルタイム課金更新メッセージの最大試行回数
Server Quiet Period (minutes)	RADIUSサーバがアクティブ状態に戻った時刻(単位は分です)
Realtime Accounting Interval (seconds)	リアルタイム課金更新メッセージの送信間隔(単位は秒です)
Stop-accounting packets buffering	RADIUS課金要求を停止するメッセージキャッシュ機能がオンの場合
Retransmission times	RADIUSを開始して課金要求を停止する最大試行回数
NAS IP Address	RADIUSメッセージを送信するNAS-IPアドレス 構成されていない場合は、Not configuredと表示されます。
Local NAS IP Address	(未サポート)自端末のDRインタフェースからアクセスするユーザのために指定した送信RADIUSメッセージが運ぶNAS-IPアドレス 指定したインタフェースのIPアドレスをNAS-IPアドレスとして使用すると、Provided by local interface xxxと表示されます。 構成されていない場合は、Not configuredと表示されます。
Peer NAS IP Address	ピアDRインタフェースからアクセスされ、そのピアにバックアップされたユーザのために指定されたRADIUSメッセージ送信用のNAS-IPアドレス 指定したインタフェースのIPアドレスをNAS-IPアドレスとして使用すると、Provided by peer interface xxxと表示されます。 構成されていない場合は、Not configuredと表示されます。
Source IP address	RADIUSメッセージの送信に使用される送信元IPアドレス 構成されていない場合は、Not configuredと表示されます。

フィールド	説明
Username format	RADIUSサーバに送信されるユーザ名の形式 • with-domain:ドメイン名を持ち運ぶ • without-domain:ドメイン名を携帯しない • keep-original:ユーザ入力との整合性
Data flow unit	データフローの単位
Packet unit	パケットの単位
Attribute 15 check-mode	次の2つの値を含む、RADIUS Attribute 15のチェック方法。 • Strict:RADIUS 標準属性値とプライベート拡張属性値を使用してチェックすることを示します。 • Loose:RADIUS 標準属性値を使用してチェックすることを示します。
Attribute 17 carry old password	(未サポート) RADIUS Attribute 17 の処理には、次の2つの値があります。 • Enabled:オンラインユーザによるパスワード変更機能が有効になっていることを示します。RADIUS 17 の属性を使用して古いパスワードを保持します。 • Disabled:ユーザパスワードのオンライン変更機能がサポートされていないことを示します。
Attribute 25	RADIUS Attribute 25の処理には、次の2つの値があります。 • Standard:RADIUS Attribute 25 が解決されないことを示します。 • CAR:RADIUS 25 属性が CAR パラメータに解決されることを示します。
Attribute 30 format	RADIUS Attribute 30の形式
Attribute 30 MAC format	RADIUS Attribute 30で伝送されるMACアドレス形式
Attribute 31 MAC format	RADIUS Attribute 31で伝送されるMACアドレス形式
Remanent-Volume threshold	ユーザ残存トラフィックのしきい値(単位はAttribute Remanent-Volume unitです。)
Attribute Remanent-Volume unit	RADIUS Remanent-Volume属性のトラフィック単位
RADIUS server version (vendor ID 2011)	2011 Vendor ID RADIUSバージョン

フィールド	説明
server-load-sharing	RADIUSサーバの負荷分散機能がオンになっている場合 • Disabled:サーバがアクティブ/パッシブモードで動作しているオフ状態 • Enabled:サーバが負荷分散モードで動作している状態
Stop-accounting-packet send-force	ユーザがオフラインの時に設備が強制的にRADIUS課金停止メッセージを送信する機能がオンの場合
Authentication response pending limit	認証サーバから応答を受信しなかった要求メッセージの最大数 構成されていない場合は、Not configuredと表示されます。
Accounting response pending limit	課金サーバが応答しなかった要求メッセージの最大数 構成されていない場合は、Not configuredと表示されます。
Username authorization	RADIUSサーバから送信されたユーザ名に対するデバイスの処理メカニズム • Applied:RADIUS サーバから送信されたユーザ名を受け入れることを示します。 • Not applied:RADIUS サーバから送信されたユーザ名を受け入れないことを示します。
All-server-block action	現在のシナリオでRADIUSサーバがすべてblockステータスになった後 • Attempt the top-priority server:現在のシナリオで優先度の高いサーバへの接続を試行します。 • Skip all servers in the scheme:現在のスキーマ内のすべてのサーバをスキップします

フィールド	説明
Attribute 218 vendor ID 25506	RADIUSメッセージ内のプライベート218属性(Vendor IDは25506です)によって運ばれるDHCP Option情報、および使用されるカプセル化フォーマット。 • Format 1 (1-byte Type field):属性をカプセル化する場合、属性の Type フィールドの長さは 1 バイトです。この方法でカプセル化された属性は、ほとんどの RADIUS サーバとの通信に適用されます。 • Format 2 (2-byte Type field):属性をカプセル化する場合、属性の Type フィールドの長さは 2 バイトです。この方法でカプセル化された属性は、HUAWEI などの特殊な RADIUS サーバと通信する RADIUS サーバに適用されます。 RADIUSメッセージにDHCP Optionプライベート属性が含まれていない場合、メッセージは表示されません。

3.3.4 display radius statistics

Syntax

display radius statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

RADIUS パケットの統計情報を表示するには、**display radius statistics** コマンドを使用します。

例

#RADIUS パケットの統計情報を表示します。

<Sysname> display radius statistics

```
                        Auth.        Acct.       SessCtrl.
Request Packet:           0            0            0
  Retry Packet:           0            0            -
Timeout Packet:           0            0            -
```

```
      Access Challenge:         0           -           -
        Account Start:          -           0           -
       Account Update:          -           0           -
         Account Stop:          -           0           -
    Terminate Request:          -           -           0
           Set Policy:          -           -           0
  Packet With Response:         0           0           0
Packet Without Response:        0           0           -
       Access Rejects:          0           -           -
       Dropped Packet:          0           0           0
       Check Failures:          0           0           0
```

表 3-5 display radius statistics コマンドの表示情報の説明

フィールド	説明
Auth.	認証パケット
Acct.	アカウンティングパケット
SessCtrl.	セッション制御パケット
Request Packet	要求パケットの数
Retry Packet	再送信された要求パケットの数
Timeout Packet	タイムアウトした要求パケットの数
Access Challenge	アクセスチャレンジパケットの数
Account Start	開始アカウンティングパケットの数
Account Update	アカウンティング更新パケットの数
Account Stop	ストップアカウンティングパケットの数
Terminate Request	ユーザを強制的にログオフするパケットの数
Set Policy	ユーザ認可情報を更新するパケットの数
Packet With Response	応答を受信したパケットの数
Packet Without Response	応答を受信しなかったパケットの数
Access Rejects	Access-Rejectパケットの数
Dropped Packet	破棄されたパケットの数
Check Failures	チェックサムエラーが発生したパケットの数

関連コマンド

reset radius statistics

3.3.5 display stop-accounting-buffer (for RADIUS)

Syntax

display stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

radius-scheme *radius-scheme-name*:RADIUS シナリオを指定する課金要求停止メッセージを示します。ここで、radius-scheme-name は RADIUS スキーマ名で、大文字と小文字を区別しない 1~32 文字の文字列です。

session-id *session-id*:指定されたセッションの課金停止要求メッセージを示します。ここで、session-id はセッション ID を表し、1~64 文字の文字列で、文字は含まれません。セッション ID:現在のオンラインユーザを一意に識別します。

time-range *start-time end-time*:指定された期間内に送信され、キャッシュされた課金停止要求メッセージを示します。ここで、start-time は要求期間の開始時間、end-time は要求期間の終了時間で、hh:mm:ss-mm/dd/yyyy (時間:分:秒-月/日/年)または hh:mm:ss-yyyy/mm/dd (時間:分:秒-年/月/日)の形式です。

user-name *user-name*:指定したユーザの課金停止要求メッセージを示す。ここで、user-name はユーザ名を表します。は 1~255 文字の文字列で、大文字と小文字が区別されます。入力したユーザ名に ISP ドメイン名を含めるかどうかは、RADIUS シナリオの user-name-format 設定と一致する必要があります。

説明

display stop-accounting-buffer コマンドは、キャッシュされた RADIUS 停止課金要求メッセージに関する情報を表示します。

例

#キャッシュされたユーザ名 abc の RADIUS 停止要求メッセージに関する情報を表示します。

<Sysname> display stop-accounting-buffer user-name abc

Total entries:2

SchemeSession IDUsernameFirst sending timeAttempts

rad 11000326232325010abc23:27:16-08/02/202019

aaa1000326232326010abc23:33:01-08/02/202020

表 3-6 display stop-accounting-buffer コマンドの表示情報の説明

フィールド	説明
Total entries:2	2つのレコードが一致します
Scheme	RADIUSスキーマ名

フィールド	説明
Session ID	セッションID (Acct-Session-Id属性値)
Username	ユーザ名
First sending time	請求停止要求が最初に送信された時刻
Attempts	課金停止要求の開始回数

関連コマンド

reset stop-accounting-buffer (for RADIUS)

retry

retry stop-accounting (for RADIUS)

stop-accounting-buffer enable (RADIUS scheme view)

user-name-format (RADIUS scheme view)

3.3.6 key (RADIUS scheme view)

Syntax

key { **accounting** | **authentication** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** }

デフォルト

RADIUS メッセージの共有キーが設定されていません。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting:RADIUS 課金メッセージの共有鍵を指定する。

authentication:RADIUS 認証メッセージの共有鍵を指定する。

cipher:キーを暗号化テキストで設定します。

simple:暗号化されたテキストとして保存されるキーをクリアテキストで設定します。

string:キー文字列。大文字と小文字が区別されます。クリアテキスト鍵が 1~64 文字の文字列;暗号文鍵は 1~117 文字の文字列である。

説明

key コマンドを使用して、RADIUS メッセージの共有キーを設定します。

undo key コマンドは、RADIUS メッセージの共有キーを削除します。

デバイスは、RADIUS 認証/課金サーバの設定時に指定されたメッセージ共有キーを優先します。この設定で指定されたメッセージ共有キーは、RADIUS 認証/課金サーバの設定時にキーが指定されていない場合にのみ使用されます。

デバイスに設定されている共有キーが RADIUS サーバのキーと完全に一致していることを確認する必要があります。

例

#RADIUS シナリオ radius1 では、課金メッセージの共有キーはクリアテキスト ok に設定されます。

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting simple ok

関連コマンド

display radius scheme

3.3.7 nas-ip (RADIUS scheme view)

Syntax

nas-ip { *ipv4-address* | **interface** *interface-type interface-number* }

undo nas-ip [**interface**]

デフォルト

RADIUS メッセージに含まれる NAS-IP アドレスが設定されていません。System view で radius nas-ip コマンドで指定された NAS-IP アドレスを使用します。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address:RADIUS メッセージに含まれる IPv4 NAS-IP アドレスを指定します。0、1、D、E、およびループバックアドレスは指定できません。

interface *interface-type interface-number*:送信元インタフェースを指定します。つまり、このインタフェースが RADIUS メッセージを送信するために使用する送信元 IP アドレスは NAS-IP アドレスです。interface-type interface-number はインターフェイスタイプおよびインタフェース番号です。

説明

nas-ip コマンドは、RADIUS メッセージに含まれる NAS-IP アドレスを設定します。

undo nas-ip コマンドは、指定されたタイプの NAS-IP アドレスを削除します。

このコマンドは、ユーザがアクセスするデバイスを識別するために使用され、RADIUS サーバ上でグローバルに一意でなければならない NAS-IP アドレスと呼ばれる、デバイスによって送信される RADIUS メッセージ内で伝送される NAS-IP-Address を構成することができる。

RADIUS サーバが送信する DAE 要求メッセージにこの属性が含まれている場合は、その要求メッセージが指定されたアクセスデバイスに送信されることを示します。アクセスデバイスが DAE 要求メッセージを受信すると、メッセージに含まれている NAS-IP アドレスとローカルに保存されている NAS-IP アドレスを比較し、同じであれば要求メッセージを受け入れて後続の処理を行い、それ以外の場合は処理しません。

物理インタフェースの障害時にサーバから返されるメッセージが到達不能にならないようにするには、送信元インタフェースとして Loopback インタフェースを使用することをお勧めします。

RADIUS scheme view と System view の両方で、RADIUS メッセージを送信する NAS-IP アドレスを次のように設定できます。

RADIUS scheme view で設定される NAS-IP アドレス(**nas-ip** コマンドを使用)は、このシナリオでのみ有効です。

System view の下の設定された NAS-IP アドレス(**radius nas-ip** コマンドを使用)はすべての RADIUS シナリオに有効です。

RADIUS scheme view の設定の優先度が高くなります。

RADIUS scheme view の下:

最大で 1 つの IPv4 NAS-IP アドレスを指定できます。

最大 1 つの送信元インタフェースを指定できます。指定した送信元インタフェースが RADIUS サーバルートに到達可能であることを確認してください。

送信元インタフェースの設定と送信元 IP アドレスの設定を同時に行うことはできません。

例

#RADIUS シナリオ radius1 で、RADIUS メッセージが運ぶ IPv4 NAS-IP アドレスを 10.1.1.1 に設定して下さい。

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] nas-ip 10.1.1.1

関連コマンド

display radius scheme

radius nas-ip

3.3.8 primary accounting (RADIUS scheme view)

Syntax

primary accounting { *host-name* | *ipv4-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

undo primary accounting

デフォルト

プライマリ RADIUS 課金サーバが設定されていません。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

host-name:プライマリ RADIUS 課金サーバのホスト名。1~253 文字の文字列で、大文字と小文字は区別されません。

ipv4-address:プライマリ RADIUS 課金サーバの IPv4 アドレス。

port-number:プライマリ RADIUS 課金サーバの UDP ポート番号。範囲は 1~65535 で、デフォルト値は 1813 です。

key:マスタ RADIUS 課金サーバとやりとりする課金メッセージの共有鍵。

cipher:キーを暗号化テキストで設定します。

simple:暗号化されたテキストとして保存されるキーをクリアテキストで設定します。

string:キー文字列。大文字と小文字が区別されます。クリアテキスト鍵が 1~64 文字の文字列;暗号文鍵は 1~117 文字の文字列である。

weight weight-value:RADIUS サーバ負荷分散の重み。weight-value はウェイト値で、0~100 の範囲で指定します。デフォルトは 0 です。0 は、負荷分散スケジュール時にサーバが使用されないことを示します。このパラメータは、サーバの負荷分散機能がオンになっている場合にのみ有効になり、重み値が大きいサーバほど多くの課金要求メッセージを処理できます。

説明

primary accounting コマンドは、プライマリ RADIUS 課金サーバを設定するために使用します。

undo primary accounting コマンドを使用して、デフォルトの状態を復元します。

設定されたプライマリ課金サーバの UDP ポート番号と課金メッセージの共有キーは、サーバの設定と一致している必要があります。

同じシナリオで指定されたプライマリ課金サーバとセカンダリ課金サーバのホスト名、IP アドレス、ポート番号は同じにすることはできません。

デバイスがプライマリ課金サーバと通信するときは、このコマンドで設定した共有キーが優先され、ここで設定しない場合は、**key accounting** コマンドで設定した共有キーが使用されます。

RADIUS サーバ負荷分散機能がオフになっているとき、課金開始要求メッセージの送信中に使用中のプライマリ課金サーバ構成が変更または削除され、そのサーバが到達不能になった場合、デバイスは現在のサーバとの通信がタイムアウトした後、優先順位の高い順に最初から順に active のサーバを探して通信します。オンラインユーザが使用している課金サーバが削除されると、ステータスが active のサーバが次の課金要求を送信しているかどうかが、優先順位の高い順に再度検出されます。

RADIUS サーバ負荷分散機能がオンの場合、課金開始要求メッセージの送信中に使用中の課金サーバ構成が変更または削除され、そのサーバが到達不能になった場合、デバイスは現在のサーバとの通信がタイムアウトした後、優先順位の高い順に最初から順に active のサーバを探して通信します。デバイスは、課金開始要求を開始したサーバとのみ通信するので、オンラインユーザが使用している課金サーバが削除される場合、デバイスは、ユーザのリアルタイム課金要求および課金停止要求を送信することができず、課金停止メッセージはローカルにキャッシュされず、これは、ユーザの課金の不正確さをもたらす。

例

#RADIUS シナリオ radius1 では、プライマリ課金サーバの IP アドレスを 10.110.1.2 に設定し、UDP ポート 1813 を使用して RADIUS 課金サービスを提供します。課金メッセージの共有キーはクリアテキスト 123456 TESTacct&!です。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813 key simple 123456TESTacct&!
```

関連コマンド

display radius scheme

key (RADIUS scheme view)

secondary accounting (RADIUS scheme view)

server-load-sharing enable

3.3.9 primary authentication (RADIUS scheme view)

Syntax

primary authentication { *host-name* | *ipv4-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

undo primary authentication

デフォルト

RADIUS プライマリ認証サーバが構成されていません。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

host-name:プライマリ RADIUS 認証サーバのホスト名。1~253 文字の文字列で、大文字と小文字は区別されません。

ipv4-address:プライマリ RADIUS 認証サーバの IPv4 アドレス。

port-number:プライマリ RADIUS 認証サーバの UDP ポート番号は、1~65535 の範囲で値を指定します。デフォルト値は 1812 です。このポート番号は、サーバが認証サービスを提供するポート番号と一致している必要があります。

key:マスタ RADIUS 認証サーバとやりとりする認証メッセージの共有鍵。この共有キーは、サーバで構成されている共有キーと一致している必要があります。

cipher:キーを暗号化テキストで設定します。

simple:暗号化されたテキストとして保存されるキーをクリアテキストで設定します。

string:キー文字列。大文字と小文字が区別されます。クリアテキスト鍵が 1~64 文字の文字列;暗号文鍵は 1~117 文字の文字列である。

test-profile *profile-name*:RADIUS サーバプローブテンプレートの名前。1~31 文字の文字列で、大文字と小文字が区別されます。

weight *weight-value*:RADIUS サーバ負荷分散の重み。weight-value はウェイト値で、0~100 の範囲で指定します。デフォルトは 0 です。0 は、負荷分散スケジュール時にサーバが使用されないことを示します。このパラメータは、サーバの負荷分散を有効にするまで有効になりません。また、重み値が大きいサーバほど、より多くの認証要求メッセージを処理できます。

説明

primary authentication コマンドは、プライマリ RADIUS 認証サーバを設定するために使用します。

undo primary authentication コマンドを使用して、デフォルトの状態を復元します。

構成されているマスタ認証サーバの UDP ポート番号と認証メッセージの共有キーは、サーバの構成と一致している必要があります。

同一のシナリオで指定したマスタ認証サーバとスレーブ認証サーバのホスト名、IP アドレス、ポート番号は同一であってはならない。

機器がマスタ認証サーバと通信する際には、このコマンドで設定した共有鍵が優先的に使用され、このコマンドで設定していない場合は、**key authenticaiton** コマンドで設定した共有鍵が使用されます。

RADIUS 認証サーバが存在するサーバプローブテンプレートを参照すると、そのサーバのプローブ機能が起動します。

RADIUS サーバの負荷分散機能がオフになっているときに、認証プロセス中に使用中のマスタ認証サーバ構成が変更または削除され、そのサーバが到達不能になった場合、デバイスは現在のサーバとの通信がタイムアウトした後、優先順位の高い順に再び active のサーバを探して通信します。

RADIUS サーバ負荷分散機能がオンになっているときに、認証プロセス中に使用中の認証サーバ構成が変更または削除され、そのサーバが到達不能になった場合、デバイスは現在のサーバとの通信タイムアウト後に、各サーバの重みとサーバによって保持されるユーザ負荷に基づいて、active のサーバとの通信を再選択します。

例

#RADIUS シナリオ radius1 で、プライマリ認証サーバの IP アドレスを 10.110.1.1 に設定し、UDP ポート 1812 を使用して RADIUS 認証/許可サービスを提供し、認証メッセージの共有キーをクリアテキスト 123456 TESTauth&!に設定します。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812 key simple 123456TESTauth&!
```

関連コマンド

display radius scheme

key (RADIUS scheme view)

radius-server test-profile

secondary authentication (RADIUS scheme view)

server-load-sharing enable

3.3.10 radius dscp

Syntax

radius dscp *dscp-value*

undo radius dscp

デフォルト

RADIUS メッセージの DSCP 優先度は 0 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value:RADIUS メッセージの DSCP 優先度。範囲は 0~63 です。値が大きいほど、優先順位が高くなります。

説明

radius dscp コマンドは、RADIUS プロトコルメッセージの DSCP プライオリティを設定するために使用します。

undo radius dscp コマンドを使用して、デフォルトの状態を復元します。

DSCP は IP メッセージ中の ToS フィールドを持ち、メッセージ自体の優先順位を表し、メッセージ転送の優先度を決定する。このコマンドでは、デバイスが送信する RADIUS メッセージが運ぶ DSCP 優先度の値を指定できる。

例

#IPv4 RADIUS メッセージの DSCP 優先順位を 10 に設定します。

<Sysname> system-view
[Sysname] radius dscp 10

3.3.11 radius nas-ip

Syntax

radius nas-ip { **interface** *interface-type interface-number* | { *ipv4-address* } }

undo radius nas-ip { **interface** | { *ipv4-address* } }

デフォルト

RADIUS メッセージに含まれる NAS-IP アドレスが設定されていない場合、デバイスは、RADIUS サーバに到達するルートアウトインターフェイスのプライマリ IPv4 アドレスを NAS-IP アドレスとして使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*:送信元インタフェースを指定します。つまり、このインタフェースが RADIUS メッセージを送信するために使用する送信元 IP アドレ

スは NAS-IP アドレスです。interface-type interface-number はインターフェイスタイプおよびインタフェース番号です。

ipv4-address:RADIUS メッセージに含まれる IPv4 NAS-IP アドレスは、自機のアドレスであるべきで、全 0 アドレス、全 1 アドレス、クラス D アドレス、クラス E アドレス、ループバックアドレスであってはならないことを指定する。

説明

radius nas-ip コマンドは、RADIUS メッセージに含まれる NAS-IP アドレスを設定します。

undo radius nas-ip コマンドは、指定されたタイプの NAS-IP アドレスを削除します。

このコマンドは、ユーザがアクセスするデバイスを識別するために使用され、RADIUS サーバ上でグローバルに一意でなければならない NAS-IP アドレスと呼ばれる、デバイスによって送信される RADIUS メッセージ内で伝送される NAS-IP-Address を構成することができる。

RADIUS サーバが送信する DAE 要求メッセージにこの属性が含まれている場合は、その要求メッセージが指定されたアクセスデバイスに送信されることを示します。アクセスデバイスが DAE 要求メッセージを受信すると、メッセージに含まれている NAS-IP アドレスとローカルに保存されている NAS-IP アドレスを比較し、同じであれば要求メッセージを受け入れて後続の処理を行い、それ以外の場合は処理しません。

物理インタフェースの障害時にサーバから返されるメッセージが到達不能にならないようにするには、送信元インタフェースとして Loopback インタフェースを使用することをお勧めします。

RADIUS scheme view と System view の両方で、RADIUS メッセージを送信する NAS-IP アドレスを次のように設定できます。

RADIUS scheme view で設定された送信元 IP アドレス(nas-ip コマンドを使用)は、この RADIUS スキーマでのみ有効です。

System view の下の設定されたソース IP アドレス(radius nas-ip コマンドを使用)はすべての RADIUS シナリオに有効です。

RADIUS scheme view の設定の優先度が高くなります。

System view では、IPv4 NAS-IP アドレスが指定できます。

System view では、最大 1 つの送信元インタフェースを指定できます。指定した送信元インタフェースが RADIUS サーバルートに到達可能であることを確認してください。

送信元インタフェースを指定する方法と IP アドレスを指定する方法の両方で設定された NAS-IP 設定は、有効になります。

例

#デバイスが RADIUS メッセージを送信するために運ぶ IPv4 NAS-IP アドレスを 129.10.10.1 に設定して下さい。

<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1

関連コマンド

nas-ip (RADIUS scheme view)

3.3.12 radius scheme

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

デフォルト

RADIUS スキーマは存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

radius-scheme-name:RADIUS スキーマの名前。1~32 文字の文字列で、大文字と小文字は区別されません。

説明

radius scheme コマンドを使用して RADIUS スキーマを作成し、RADIUS scheme view に移動します。指定した RADIUS スキーマがすでに存在する場合は、RADIUS scheme view に直接移動します。

undo radius scheme コマンドは、指定された RADIUS スキーマを削除するために使用します。

1 つの RADIUS シナリオは､複数の ISP ドメインによって同時に参照することができる。

システムは最大 16 個の RADIUS シナリオをサポートします。

例

#radius1 という名前の RADIUS スキーマを作成し、ビューに移動します。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

関連コマンド

display radius scheme

3.3.13 radius-server test-profile

Syntax

radius-server test-profile *profile-name* **username** *name* **[interval** *interval* **]**

undo radius-server test-profile *profile-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: テストプロファイルの名前を指定します。大文字と小文字を区別します。文字数は 1～31 文字です。

username *name*: 検出パケット内のユーザ名を指定します。name パラメータは大文字と小文字を区別し、1～253 文字で指定します。

interval *interval*: 検出パケットを送信する間隔を分で設定します。interval パラメータの値の範囲は 1～3600 で、デフォルトは 60 です。

説明

radius-server test-profile コマンドは RADIUS サーバの状態を検出するためのテストプロファイルを設定します。

undo radius-server test-profile コマンドはテストプロファイルを削除します。

装置は、サーバに対して指定されたテストプロファイルが存在する場合にのみ、RADIUS サーバの状態検出を開始します。存在しないテストプロファイルを RADIUS サーバに対して指定した場合、装置上にテストプロファイルを作成するまで、装置はサーバの状態を検出しません。

テストプロファイルを削除すると、装置は削除したテストプロファイルを使用していた RADIUS サーバの状態の検出を停止します。

このコマンドを複数回実行することで、複数のテストプロファイルを設定できます。

例

RADIUS サーバの状態を検出するためにテストプロファイル abc を設定します。ユーザ名 admin を使用した検出パケットを 10 分ごとに送信します。

```
<AC> system-view
[AC] radius-server test-profile abc username admin interval 10
```

関連コマンド

primary authentication (RADIUS scheme view)

secondary authentication (RADIUS scheme view)

3.3.14 reauthentication server-select

Syntax

reauthentication server-select { **inherit** | **reselect** }

undo reauthentication server-select

デフォルト

Inherit モード

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

inherit: 認証を行った RADIUS サーバを再認証に使用します。

reselect: 再認証用の RADIUS サーバを再選択します。

説明

このコマンドを使用して、再認証時の RADIUS サーバ選択メカニズムを設定します。ネットワークの状態に応じて、次のいずれかのモードを使用します。

inherit:デバイスは、ユーザの認証を実行した RADIUS サーバを使用して、そのユーザを再認証します。このモードでは、再認証に使用される時間が短縮されます。ただし、RADIUS サーバに到達できない場合、再認証は失敗します。

reselect :デバイスは、到達可能な RADIUS サーバを検索してユーザを再認証します。このモードは、継承モードよりも時間がかかります。ただし、このモードでは、デバイスは再認証に最適な到達可能な RADIUS サーバを使用します。RADIUS サーバの選択には、次の要素が影響します。

- RADIUS スキームのサーバ設定 (設定順を含む) 。
- RADIUS スキームの RADIUS サーバのステータス。

例

#RADIUS scheme radius1 で、RADIUS サーバの選択モードを reselect に設定する。

<Sysname> system-view
[Sysname] radius scheme radius1

[Sysname-radius-radius1] reauthentication server-select reselect

関連コマンド

display radius scheme

3.3.15 reset radius statistics

Syntax

reset radius statistics

View

User view

定義済みユーザロール

network-admin

例

#RADIUS プロトコルの統計情報をクリアします。

<Sysname> reset radius statistics

関連コマンド

display radius statistics

3.3.16 reset stop-accounting-buffer (for RADIUS)

Syntax

reset stop-accounting-buffer { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time end-time* | **user-name** *user-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

radius-scheme *radius-scheme-name*:RADIUS シナリオを指定した停止課金応答メッセージを示します。ここで、radius-scheme-name は RADIUS スキーマ名で、大文字と小文字を区別しない 1~32 文字の文字列です。

session-id *session-id*:指定されたセッションの停止課金応答メッセージを示します。ここで、session-id はセッション ID を表し、1~64 文字の文字列で、文字は含まれません。セッション ID:現在のオンラインユーザを一意に識別します。

time-range *start-time end-time*:指定された期間内に送信され、キャッシュされた課金停止要求メッセージを示します。ここで、start-time は要求期間の開始時間です。end-time は、要求された期間の終了時刻で、hh:mm:ss-mm/dd/yyyy (時間:分:秒-月/日/年)または hh:mm:ss-yyyy/mm/dd (時間:分:秒-年/月/日)の形式です。

user-name *user-name*:指定したユーザ名の課金停止応答メッセージを表示する。ここで、user-name はユーザ名を表します。は 1~255 文字の文字列で、大文字と小文字が区別されます。入力したユーザ名が ISP ドメイン名を持つかどうかは、RADIUS スキーマに設定されている RADIUS サーバに送信されるユーザ名の形式と一致する必要があります。

説明

reset stop-accounting-buffer コマンドキャッシュをクリアするために使用される RADIUS 課金要求メッセージを停止します。

例

#キャッシュをクリアしたユーザ user0001@test の RADIUS 課金要求メッセージを停止します。

<Sysname> reset stop-accounting-buffer user-name user0001@test

#2020 年 1 月 31 日 0:00:00 から 2020 年 1 月 31 日 23:59:59 までの間にキャッシュされた課金停止要求メッセージをクリアします。

<Sysname> reset stop-accounting-buffer time-range 00:00:00-01/31/2020 23:59:59-01/31/2020

関連コマンド

display stop-accounting-buffer (for RADIUS)
stop-accounting-buffer enable (RADIUS scheme view)

3.3.17 retry

Syntax

retry *retries*

undo retry

デフォルト

RADIUS メッセージを送信する最大試行回数は 3 回である。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries:RADIUS メッセージを送信する最大試行回数。範囲は 1~20 です。

説明

retry コマンドは、RADIUS メッセージを送信する最大試行回数を設定します。

undo retry コマンドを使用して、デフォルトの状態を復元します。

RADIUS プロトコルは UDP メッセージを使用してデータを伝送するため、通信プロセスは信頼性に欠けます。デバイスが応答タイムアウトタイマーによって指定された時間内(**timer response-timeout** コマンドで設定)に RADIUS サーバから応答を受信しない場合、デバイスは RADIUS 要求メッセージを RADIUS サーバに再送信する必要があります。累積転送回数が最大転送回数に達しても RADIUS サーバが応答しない場合、デバイスはこの要求を失敗と見なします。

次の点に注意してください。

RADIUS メッセージを送信する最大試行回数、RADIUS サーバの応答タイムアウト時間、および設定されている RADIUS サーバの合計数は、アクセスモジュールで定義されているユーザ認証タイムアウト時間を超えないようにしてください。そうしないと、RADIUS 認証プロセスが完了する前にユーザが強制的にオフラインにされる可能性があります。

デバイスは、構成された順序で次の RADIUS サーバとの通信を試行する前に、現在の累積試行時間が 300 秒以上かどうかを判断します。300 秒以上になると、RADIUS 要求メッセージは次の RADIUS サーバに送信されなくなり、RADIUS 要求の送信は失敗したとみなされます。したがって、このタイムアウトメカニズムのために、展開された RADIUS サーバの一部がに使用できなくなるのを防ぐには、設定された RADIUS サーバの合計数に基づいて、RADIUS メッセージを送信する最大試行回数と RADIUS サーバの応答タイムアウト時間を適切に設定することをお勧めします。

例

#RADIUS シナリオ radius1 で、RADIUS メッセージを送信する最大試行回数を 5 回に設定します。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

関連コマンド

radius scheme
timer response-timeout (RADIUS scheme view)

3.3.18 retry realtime-accounting

Syntax

retry realtime-accounting *retries*

undo retry realtime-accounting

デフォルト

デバイスがリアルタイム課金要求を開始できる最大試行回数は 5 です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries:リアルタイム課金要求の開始を許可される試行の最大数。1~255 の値をとります。

説明

retry realtime-accounting コマンドを使用して、リアルタイム課金要求の開始を許可する最大試行回数を設定します。

undo retry realtime-accounting コマンドを使用して、デフォルトの状態を復元します。

RADIUS サーバは通常、接続タイムアウトタイマーを使用して、ユーザがオンラインであるかどうかを判断します。RADIUS サーバが接続タイムアウト時間内にデバイスからのリアルタイム課金メッセージを受信できない場合、サーバは回線またはデバイスに障害があると見なし、ユーザのアカウンティングを停止します。このような RADIUS サーバの特性に合わせて、不測の障害が発生した場合には、デバイス側と RADIUS サーバが同期してユーザの接続を切断するようにする必要がある。デバイスは、RADIUS サーバへの接続がタイムアウトした場合に、デバイスが RADIUS サーバへのリアルタイム課金要求をできる限り長く試行することを保証するために、リアルタイム課金要求に対する連続した無応答回数制限の設定を提供する。デバイスが設定された制限を超えて応答を受信しない場合、ユーザ接続は切断されます。

RADIUS サーバの応答タイムアウト時間(**timer response-timeout** コマンドの設定)が 3 秒で、RADIUS メッセージを送信する最大試行回数(retry コマンドの設定)が 3 回で、設備のリアルタイム課金間隔(**timer realtime-accounting** コマンドの設定)が 12 分で、設備が許可するリアルタイム課金無応答の最大回数が 5 回(**retry realtime-accounting** コマンドの設定)であると仮定すると、その意味は以下のとおりである:設備は 12 分ごとに課金要求を起動し、3 秒で応答が得られなければ再度要求を起動し、3 回の送信で応答が得られなければそのリアルタイム課金は失敗したと見なし、その後 12 分ごとに再度送信し、5 回とも失敗した後、設備はユーザ接続を切断する。

例

#RADIUS シナリオ radius1 で、リアルタイム課金要求の開始を許可する最大試行回数を 10 に設定します。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry realtime-accounting 10
```

関連コマンド

retry
timer realtime-accounting (RADIUS scheme view)
timer response-timeout (RADIUS scheme view)

3.3.19 retry stop-accounting (RADIUS scheme view)

Syntax

retry stop-accounting *retries*

undo retry stop-accounting

デフォルト

RADIUS の課金要求を停止する最大試行回数は 500 回です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries:停止要求が応答しない最大回数。値の範囲は 10~65535 です。

説明

retry stop-accounting コマンドは、RADIUS 停止課金要求を開始する最大試行回数を設定します。

undo retry stop-accounting コマンドを使用して、デフォルトの状態を復元します。

デバイスは、RADIUS 停止課金要求の最大試行回数を開始することによって、他の関連パラメータとともに停止課金要求メッセージの送信を制御する。次の構成が想定されます。

RADIUS サーバの応答タイムアウト時間(**timer response-timeout** コマンドで設定)は 3 秒;

RADIUS メッセージ送信の最大試行回数(**retry** コマンドで設定)は 5;

応答のない RADIUS の課金要求メッセージのキャッシュを無効にする;

デバイスが課金停止要求を開始する最大試行回数は 20 回です(**retry stop-accounting** コマンドで設定)。

そして、デバイスが課金停止要求メッセージを送信してから 3 秒以内にサーバからの応答がなければそのメッセージを再送する。デバイスが 5 回送信しても応答しない場合は、そのメッセージがデバイスにキャッシュされ、課金停止要求が再度開始されます。20 回の要求試行がすべて失敗した後、デバイスはキャッシュされたメッセージを廃棄します。

例

#RADIUS シナリオ radius1 で、RADIUS 停止課金要求を開始する最大試行回数を 1000 に設定します。

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000

関連コマンド

display stop-accounting-buffer (for RADIUS)
retry
timer response-timeout (RADIUS scheme view)

3.3.20 secondary accounting (RADIUS scheme view)

Syntax

secondary accounting { *host-name* | *ipv4-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

undo secondary accounting [{ *host-name* | *ipv4-address* } [*port-number*]]

デフォルト

RADIUS からの課金サーバは設定されません。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

host-name:RADIUS から課金されるサーバのホスト名。1~253 文字の文字列で、大文字と小文字は区別されません。

ipv4-address:RADIUS からサーバの IPv4 アドレスを請求します。

port-number:RADIUS 課金サーバの UDP ポート番号から、1～65535 の範囲で値をとり、デフォルト値は 1813 である。

key:RADIUS 課金サーバとやり取りする課金メッセージの共有キー。

cipher:キーを暗号化テキストで設定します。

simple:暗号化されたテキストとして保存されるキーをクリアテキストで設定します。

string:キー文字列。大文字と小文字が区別されます。クリアテキスト鍵が 1~64 文字の文字列;暗号文鍵は 1~117 文字の文字列である。

weight *weight-value*:RADIUS サーバ負荷分散の重み。weight-value はウェイト値で、0~100 の範囲で指定します。デフォルトは 0 です。0 は、負荷分散スケジュール時にサーバが使用されないことを示します。このパラメータは、サーバの負荷分散機能がオンになっている場合にのみ有効になり、重み値が大きいサーバほど多くの課金要求メッセージを処理できます。

説明

secondary accounting コマンドは RADIUS からの課金サーバを設定するのに使用されます。

undo secondary accounting コマンドは RADIUS から指定された課金サーバを削除するのに使用されます。

設定される課金サーバからの UDP ポート番号および課金メッセージのための共有キーはサーバの設定と一致する必要があります。

各 RADIUS シナリオでは、RADIUS からの課金サーバを 16 台まで設定できます。マスターサーバに到達できない場合、デバイスは、スレーブサーバが設定されている順序に基づいて、ステータスが active のスレーブサーバを最初から最後まで探し、操作します。

同一のシナリオで指定されたマスタ課金サーバとスレーブ課金サーバのホスト名、IP アドレス、ポート番号は同一であってはならず、各スレーブ課金サーバのホスト名、IP アドレス、ポート番号も同一であってはならない。

デバイスが課金サーバと通信する場合は、このコマンドで設定した共有キーが優先的に使用され、ここで設定しない場合は、**key accounting** コマンドで設定した共有キーが使用されます。

RADIUS サーバ負荷分散機能がオフの場合、課金開始要求メッセージの送信中に使用中のスレーブサーバ構成が変更または削除され、サーバが到達不能になった場合、デバイスは現在のサーバとの通信がタイムアウトした後、優先順位の高い順に最初から順に active のサーバを探して通信します。オンラインユーザが使用している課金サーバが削除されると、ステータスが active のサーバが次の課金要求を送信しているかどうかが、優先順位の高い順に再度検出されます。

RADIUS サーバ負荷分散機能がオンの場合、課金開始要求メッセージの送信中に使用中の課金サーバ構成が変更または削除され、そのサーバが到達不能になった場合、デバイスは現在のサーバとの通信がタイムアウトした後、優先順位の高い順に最初から順に active のサーバを探して通信します。デバイスは、課金開始要求を開始したサーバとのみ通信するので、オンラインユーザが使用している課金サーバが削除される場合、デバイスは、ユーザのリアルタイム課金要求および課金停止要求を送信することができず、課金停止メッセージはローカルにキャッシュされない。

例

#RADIUS シナリオ radius1 では、UDP ポート 1813 を使用して RADIUS 課金サービスを提供するために、課金サーバからの IP アドレスを 10.110.1.1 に設定します。

```
<Sysname> system-view
[Sysname] radius scheme radius1
```

[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813

#RADIUS シナリオ radius2 では、IP アドレス 10.110.1.1、10.110.1.2 の 2 つのスレーブ課金サーバを設定し、両方とも UDP ポート 1813 を使用して RADIUS 課金サービスを提供します。

<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary accounting 10.110.1.1 1813
[Sysname-radius-radius2] secondary accounting 10.110.1.2 1813

関連コマンド

display radius scheme
key (RADIUS scheme view)
primary accounting

3.3.21 secondary authentication (RADIUS scheme view)

Syntax

secondary authentication { *host-name* | *ipv4-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

undo secondary authentication [{ *host-name* | *ipv4-address* } [*port-number*]]

デフォルト

RADIUS 認証サーバから設定されていません。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

host-name:RADIUS からの認証サーバのホスト名で、大文字と小文字を区別しない 1~253 文字の文字列。

ipv4-address:RADIUS 認証サーバからの IPv4 アドレス。

port-number:RADIUS 認証サーバの UDP ポート番号から、1～65535 の範囲で値をとり、デフォルト値は 1812 である。

key:RADIUS 認証サーバとやりとりする認証メッセージの共有鍵。

cipher:キーを暗号化テキストで設定します。

simple:暗号化されたテキストとして保存されるキーをクリアテキストで設定します。

string:キー文字列。大文字と小文字が区別されます。クリアテキスト鍵が 1~64 文字の文字列;暗号文鍵は 1~117 文字の文字列である。

test-profile *profile-name*:RADIUS サーバプローブテンプレートの名前。1~31 文字の文字列で、大文字と小文字が区別されます。

weight *weight-value*:RADIUS サーバ負荷分散の重み。weight-value はウェイト値で、0~100 の範囲で指定します。デフォルトは 0 です。0 は、負荷分散スケジュール時にサーバが使用されないことを示します。このパラメータは、サーバの負荷分散を有効にするまで有効になりません。また、重み値が大きいサーバほど、より多くの認証要求メッセージを処理できます。

説明

secondary authentication コマンドは RADIUS 認証サーバから設定するのに使用されます。

undo secondary authentication コマンドは RADIUS から指定された認証サーバを削除するのに使用されます。

設定される認証サーバからの UDP ポート番号および認証メッセージの共有キーはサーバの設定と一致する必要があります。

各 RADIUS シナリオでは、RADIUS 認証サーバから最大 16 台の設定がサポートされています。マスターサーバに到達できない場合、デバイスは、スレーブサーバが設定されている順序に基づいて、ステータスが active のスレーブサーバを最初から最後まで探し、操作します。

RADIUS 認証サーバが存在するサーバプローブテンプレートを参照すると、そのサーバのプローブ機能が起動します。

同一のシナリオで指定したマスタ認証サーバとスレーブ認証サーバのホスト名、IP アドレス、ポート番号は同一であってはならず、また、各スレーブ認証サーバのホスト名、IP アドレス、ポート番号も同一であってはならない。

機器が認証サーバと通信する場合は、このコマンドで設定した共有鍵が優先的に使用され、ここで設定していない場合は、**key authentication** コマンドで設定した共有鍵が使用されます。

RADIUS サーバの負荷分散機能がオフになっているときに、使用中のスレーブサーバ構成が認証中に変更または削除され、そのサーバが到達不能になった場合、デバイスは現在のサーバとの通信がタイムアウトした後、優先順位の高い順に再び active のサーバを探して通信します。

RADIUS サーバ負荷分散機能がオンになっているときに、認証プロセス中に使用中の認証サーバ構成が変更または削除され、そのサーバが到達不能になった場合、デバイスは現在のサーバとの通信タイムアウト後に、各サーバの重みとサーバによって保持されるユーザ負荷に基づいて、active のサーバとの通信を再選択します。

例

#RADIUS シナリオ radius1 では、認証サーバからの IP アドレスを 10.110.1.2 に設定し、UDP ポート 1812 を使用して RADIUS 認証/許可サービスを提供します。

```
<Sysname> system-view
[Sysname] radius scheme radius1
```

[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812

#RADIUS シナリオ radius2 では、IP アドレス 10.110.1.1、10.110.1.2 の 2 つのスレーブ認証サーバを設定し、両方とも UDP ポート 1812 を使用して RADIUS 認証/許可サービスを提供します。

<Sysname> system-view
[Sysname] radius scheme radius2
[Sysname-radius-radius2] secondary authentication 10.110.1.1 1812
[Sysname-radius-radius2] secondary authentication 10.110.1.2 1812

関連コマンド

display radius scheme

key (RADIUS scheme view)

primary authentication (RADIUS scheme view)

radius-server test-profile

3.3.22 snmp-agent trap enable radius

Syntax

snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

undo snmp-agent trap enable radius [**accounting-server-down** | **accounting-server-up** | **authentication-error-threshold** | **authentication-server-down** | **authentication-server-up**] *

デフォルト

すべてのタイプの RADIUS アラーム機能はオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

accounting-server-down:RADIUS 課金サーバ到達可能状態が down になったときに警告メッセージを送信することを示す。

accounting-server-up:RADIUS 課金サーバ到達可能状態が up になったときに警告メッセージを送信することを示す。

authentication-error-threshold:認証失敗回数が閾値を超えた場合に警告メッセージを送信することを示す。このしきい値は、認証要求総数に対する認証失敗回数の割合の値で、現時点では MIB 方式のみで構成でき、1~100 の値をとり、デフォルトは 30 である。

authentication-server-down:RADIUS 認証サーバ到達可能状態が down になったときに警告メッセージを送信することを示す。

authentication-server-up:RADIUS 認証サーバ到達可能状態が up になったときに警告メッセージを送信することを示す。

説明

snmp-agent trap enable radius コマンドは、RADIUS アラーム機能をオンにするために使用します。

undo snmp-agent trap enable radius コマンドを使用して、指定した RADIUS アラーム機能をオフにします。

パラメータを指定しない場合は、すべてのタイプの RADIUS アラーム機能がオンまたはオフになります。

RADIUS サーバーアラーム機能を有効にすると、次のようなアラーム情報が生成されます。

RADIUS サーバ到達不能アラーム:NAS から RADIUS サーバに課金要求が送信されたとき、または認証要求が応答を受信しなかったときに、要求が再送されます。このアラームは、再送回数が最大転送回数に達しても応答がない場合に送信されます。

RADIUS サーバ到達可能アラーム:timer quiet タイマーで設定した時間が経過すると、NAS はサーバの状態をアクティブにしてアラームを送信します。

認証失敗数がしきい値を超えた場合のアラート:NAS は、認証要求の総数に対する認証失敗数の割合がしきい値を超えたことを検出すると、このアラート情報を送信します。

例

#オン RADIUS 課金サーバ到達可能状態が down になったときのアラーム機能。

<Sysname> system-view
[Sysname] snmp-agent trap enable radius accounting-server-down

3.3.23 state primary

Syntax

state primary { **accounting** | **authentication** } { **active** | **block** }

デフォルト

プライマリ RADIUS サーバのステータスは active です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting:プライマリ RADIUS 課金サーバ。

authentication:プライマリ RADIUS 認証サーバ。

active:通常の動作状態。

block:通信が中断された状態。

説明

state primary コマンドは、プライマリ RADIUS サーバのステータスを設定します。

RADIUS サーバ負荷分担機能がオフ状態にある時、毎回ユーザは認証或は課金を開始して、もし主サーバの状態が active であれば、設備はまず主サーバと通信を試みて、もし主サーバが到達不能であれば、主サーバの状態を block に設定して、同時に主サーバの timer quiet タイマーを起動して、その後設備は厳格に従サーバの配置順序に従って順次に状態が active の従サーバを探す。timer quiet タイマーによって設定された時間が経過すると、プライマリ・サーバの状態は block から active に戻ります。タイマーが期限切れになる前に、このコマンドを使用してマスターサーバの状態を手動で block に設定すると、タイマーが期限切れになっても、マスターサーバの状態は、このコマンドを使用して手動で active に設定しない限り、自動的に active に戻りません。

RADIUS サーバ負荷分散機能がオンになっている場合、デバイスは、現在各サーバによってホストされているユーザ負荷スケジューリング状態が active であるサーバからのみ認証または課金要求を送信する。

マスタとすべてのスレーブのステータスが block の場合、認証または課金にはマスタが使用されます。

認証サーバの状態は、サーバへのデバイスの到達可能性プローブ機能のオンに影響します。指定されたサーバの状態が active で、そのサーバが **radius-server test-profile** コマンドを使用して既存のサーバプローブテンプレートを正常に参照した場合、デバイスはそのサーバの到達可能性プローブを有効にします。サーバの到達可能性プローブは、手動でサーバの状態を block に設定するとオフになります。

例

#RADIUS シナリオ radius1 で、プライマリ認証サーバのステータスを block に設定します。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state primary authentication block
```

関連コマンド

display radius scheme

radius-server test-profile

server-load-sharing enable

state secondary

3.3.24 state secondary

Syntax

state secondary { **accounting** | **authentication** } [{ *host-name* | *ipv4-address* } [*port-number*]] { **active** | **block** }

デフォルト

RADIUS からサーバステータスは active です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting:RADIUS からサーバを請求します。

authentication:RADIUS からサーバを認証します。

host-name:RADIUS サーバのホスト名から、大文字と小文字を区別しない 1~253 文字の文字列。

ipv4-address:RADIUS サーバからの IPv4 アドレス。

port-number:RADIUS サーバからの UDP ポート番号は、1~65535 の範囲をとり、RADIUS 課金サーバからのデフォルト UDP ポート番号は 1813, RADIUS 認証サーバからのデフォルト UDP ポート番号は 1812 である。

active:通常の動作状態。

block:通信が中断された状態。

説明

state secondary コマンドは RADIUS サーバからのステータスを設定するのに使用されます。

スレーブ IP アドレスを指定しない場合、このコマンドは設定されたすべてのスレーブ認証サーバまたはスレーブ課金サーバのステータスを変更します。

RADIUS サーバの負荷分散機能がオフになっているときに、デバイスが active というステータスのスレーブサーバに到達できないことを検出すると、デバイスはそのスレーブサーバのステータスを block に設定し、サーバの timer quiet タイマーを開始して、次の active というステータスのスレーブサーバの検出を続行します。timer quiet タイマーで設

定した時間になると、スレーブ状態は block から active に回復する。タイマーがタイムアウトする前に、このコマンドを使用してスレーブサーバの状態を block に手動で設定すると、タイマーがタイムアウトしても、スレーブサーバの状態は、このコマンドを使用して active に手動で設定しない限り、自動的に active に戻りません。構成済みのすべてのスレーブサーバに到達できない場合、この認証または課金は失敗します。

RADIUS サーバ負荷分散機能がオンになっている場合、デバイスは、現在各サーバによってホストされているユーザ負荷スケジューリング状態が active であるサーバからのみ認証または課金要求を送信する。

認証サーバの状態は、サーバへのデバイスの到達可能性プローブ機能のオンに影響します。指定されたサーバの状態が active で、そのサーバが radius-server test-profile コマンドを使用して既存のサーバプローブテンプレートを正常に参照した場合、デバイスはそのサーバの到達可能性プローブを有効にします。サーバの到達可能性プローブは、手動でサーバの状態を block に設定するとオフになります。

例

#RADIUS シナリオ radius1 では、認証サーバからの状態を block に設定します。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication block
```

関連コマンド

display radius scheme
radius-server test-profile
server-load-sharing enable
state primary

3.3.25 stop-accounting-buffer enable (RADIUS scheme view)

Syntax

stop-accounting-buffer enable

undo stop-accounting-buffer enable

デフォルト

デバイスキャッシュが応答しない RADIUS 課金要求メッセージを停止します。

View

RADIUS scheme view

定義済みユーザロール

network-admin

説明

stop-accounting-buffer enable コマンドは、応答のない RADIUS 停止要求メッセージのキャッシュを有効にします。

undo stop-accounting-buffer enable コマンドは、応答のない RADIUS に対する課金要求メッセージのキャッシュ機能を停止するために使用されます。

デバイスが課金停止要求メッセージを送信し、RADIUS サーバが応答しない場合、デバイスは retry コマンドで設定された最大試行回数でメッセージの再送信を試みます。デバイスがこの RADIUS メッセージを送信する最大試行回数が最大値を超えても応答しない場合、この機能がオンになっていると、デバイスはメッセージをキャッシュしてから再度要求を発行し、応答しない場合は、上記の手順を繰り返し、一定回数(**retry stop-accounting** コマンドで設定)経過すると、デバイスはメッセージを廃棄します。

RADIUS スキーマの課金サーバが削除されると、デバイスは対応するキャッシュされた課金停止要求メッセージを破棄します。

例

#応答のない RADIUS 課金要求メッセージのキャッシュを無効にします。

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable

関連コマンド

display stop-accounting-buffer (for RADIUS)
reset stop-accounting-buffer (for RADIUS)

3.3.26 timer quiet (RADIUS scheme view)

Syntax

timer quiet *minutes*

undo timer quiet

デフォルト

サーバがアクティブになるまでの時間は 5 分です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

minutes:アクティブな状態に戻る時間。1~255 の値を分単位で指定できます。

説明

timer quiet コマンドは、サーバがアクティブ状態に戻る時間を設定します。

undo timer quiet コマンドを使用して、デフォルトの状態を復元します。

サーバをアクティブ状態に戻す時間を適切に設定することをお勧めします。

サーバがアクティブ状態に復帰するまでの時間を短く設定しすぎると、デバイスが状態 active で実際には到達不能なサーバと通信しようとして認証または課金が頻繁に失敗するという問題が発生します。

サーバがアクティブ状態に復帰するまでの時間を長く設定しすぎると、サーバが正常に復帰した後に、デバイスと通信できなくなり、ユーザの認証や課金の効率が低下します。

例

#RADIUS シナリオ radius1 で、サーバがアクティブ状態に戻るまでの時間を 10 分に設定します。

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer quiet 10

関連コマンド

display radius scheme

3.3.27 timer realtime-accounting (RADIUS scheme view)

Syntax

timer realtime-accounting *interval* [**second**]

undo timer realtime-accounting

デフォルト

リアルタイム課金の時間間隔は 12 分。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

interval:0~71582 の範囲でリアルタイムに課金される時間間隔。

second:リアルタイムで課金される時間間隔は秒単位で、デフォルトは分単位です。

説明

timer realtime-accounting コマンドを使用して、リアルタイム課金の間隔を設定します。

undo timer realtime-accounting コマンドを使用して、デフォルトの状態を復元します。

ユーザにリアルタイム課金を実施するには、リアルタイム課金の時間間隔を設定する必要がある。値を取得する処理は、次のように異なります。

リアルタイム課金間隔が 0 でない場合、デバイスは、設定された時間ごとにオンラインユーザの課金情報を RADIUS サーバに送信する。

リアルタイム課金間隔が 0 に設定され、サーバ上にリアルタイム課金間隔が構成されている場合、デバイスは、サーバ上に構成されたリアルタイム課金間隔に従って、オンラインユーザの課金情報を RADIUS サーバに送信する。サーバで値が設定されていない場合、アプライアンスはオンラインユーザの課金情報を RADIUS サーバに送信しません。

リアルタイムの課金間隔の値は小さく、課金の正確性は高いが、設備と RADIUS サーバに対する性能要求は高い。

表 3-7 リアルタイム課金間隔とユーザボリューム間の推奨比例関係

ユーザ数	リアルタイムチャージバック間隔(分)
1~99	3
100~499	6
500~999	12
1000以上	15以上

RADIUS の認証と認可を行わず、RADIUS の課金のみを行うユーザは、課金スキームで設定されたリアルタイム課金間隔のみを使用でき、RADIUS サーバで設定されたリアルタイム課金間隔は使用できません。

例

#RADIUS シナリオ radius1 で、リアルタイム課金の間隔を 51 分に設定する。

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51

関連コマンド

retry realtime-accounting

3.3.28 timer response-timeout (RADIUS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

デフォルト

RADIUS サーバのレスポンスタイムアウトは 3 秒です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

seconds:RADIUS サーバのレスポンスタイムアウト時間。1~10 の範囲で秒単位で指定します。

説明

timer response-timeout コマンドは、RADIUS サーバのレスポンスタイムアウト時間を設定します。

undo timer response-timeout コマンドを使用して、デフォルトの状態を復元します。

RADIUS 要求メッセージが送信されてからしばらく経過しても、デバイスが RADIUS サーバから応答を受信しない場合は、RADIUS 要求メッセージを再送する必要があります。これは、ユーザができる限り RADIUS サービスを利用できるようにするための時間で、RADIUS サーバ応答タイムアウトと呼ばれます。このコマンドでは、この時間を調整します。

次の点に注意してください。

RADIUS メッセージを送信する最大試行回数、RADIUS サーバの応答タイムアウト時間、および設定されている RADIUS サーバの合計数は、アクセスモジュールで定義されているユーザ認証タイムアウト時間を超えないようにしてください。そうしないと、RADIUS 認証プロセスが完了する前にユーザが強制的にオフラインにされる可能性があります。

デバイスは、構成された順序で次の RADIUS サーバとの通信を試行する前に、現在の累積試行時間が 300 秒以上かどうかを判断します。300 秒以上になると、RADIUS 要求メッセージは次の RADIUS サーバに送信されなくなり、RADIUS 要求の送信は失敗したとみなされます。したがって、このタイムアウトメカニズムのために、展開された RADIUS サーバの一部が使用できなくなるのを防ぐには、設定された RADIUS サーバの合計数に基づいて、RADIUS メッセージを送信する最大試行回数と RADIUS サーバの応答タイムアウト時間を適切に設定することをお勧めします。

例

#RADIUS シナリオ radius1 で、サーバ応答タイムアウトを 5 秒に設定します。

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

関連コマンド

display radius scheme
retry

3.3.29 user-name-format (RADIUS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

undo user-name-format

デフォルト

RADIUS サーバに送信されるユーザ名は、ISP ドメイン名を保持します。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

keep-original:RADIUS サーバに送信されるユーザ名は、ユーザの入力と一致する。

with-domain:RADIUS サーバに送信されるユーザ名は ISP ドメイン名を運ぶ。

without-domain:RADIUS サーバに送信されるユーザ名は ISP ドメイン名を持っていません。

説明

user-name-format コマンドは、RADIUS サーバに送信するユーザ名の形式を設定します。

undo user-name-format コマンドを使用して、デフォルトの状態を復元します。

アクセスするユーザの名前は通常「userid@isp-name」の形式で、「@」の後に ISP のドメイン名が続くが、デバイスはこのドメイン名からユーザをどの ISP のドメインに所属させるかを決める。しかし、初期の RADIUS サーバの中には ISP のドメイン名を携帯しているユーザ名を受け入れることができないものがあり、その場合、ユーザ名に携帯しているドメイン名を取り除いて RADIUS サーバに転送する必要がある。そのため、アプライアンスはこのコマンドを提供して、RADIUS サーバに送信されるユーザ名が ISP ドメイン名を持つかどうかを指定します。

ユーザ名に ISP ドメイン名を含めない RADIUS スキームを指定する場合は、複数の ISP ドメインで RADIUS スキームを使用するように設定しないでください。そうしないと、実際のユーザは異なりますが(別の ISP ドメイン内)、RADIUS サーバはユーザを同じ(転送先のユーザ名が同じであるため)とみなすというエラーが発生します。

802.1 X ユーザが EAP 認証方式の場合、 RADIUS スキームで設定された **user-name-format** コマンドは無効であり、クライアントが RADIUS サーバに渡すユーザ名はユーザが入力したユーザ名と一致する。

アクセスユーザがローミングを必要とするワイヤレスユーザである場合は、RADIUS サーバに送信されるユーザ名の形式を keep-original タイプに設定することをお勧めします。設定しないと、このタイプのユーザ認証が失敗する可能性があります。

例

#RADIUS シナリオ radius1 では、RADIUS サーバに送信されるユーザ名にドメイン名を付けないように設定します。

<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain

関連コマンド

display radius scheme

3.4 EAPプロファイル設定コマンド

🕮 **メモ：**

この機能は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

3.4.1 ca-file

Syntax

ca-file *file-name*

undo ca-file

デフォルト

EAP 認証のための CA 証明書が指定されていません。

View

EAP profile view

定義済みユーザロール

network-admin

パラメータ

file-name: CA 証明書ファイル名を指定します。大文字と小文字を区別する 1～91 文字の文字列です。PEM 形式の CA 証明書ファイルのみをサポートします。

説明

ca-file コマンドは、EAP 認証のための CA 証明書ファイルを指定します。

undo ca-file コマンドを使用して、デフォルトの状態を復元します。

PEAP-MSCHAPv2、TTLS-MSCHAPv2 の EAP 認証方式を使用する場合、RADIUS クライアントの証明書を認証するために、RADIUS サーバに CA 証明書ファイルを指定する必要があります。

CA 証明書ファイルを指定する前に、FTP または TFTP を使用して、そのファイルをデバイスのデフォルトストレージメディアのルートディレクトリに転送する必要があります。クラウドクラスタの場合、各メンバーデバイスのデフォルトストレージメディアのルートディレクトリにファイルが既に存在していることを確認してください。

EAP プロファイルには CA 証明書ファイルを 1 つだけ指定できます。このコマンドを複数回実行した場合、最新の設定が有効になります。

例

#EAP プロファイル eap1 で、EAP 認証用の CA 証明書ファイル ca.pem を指定します。

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] ca-file ca.pem
```

3.4.2 certificate-file

Syntax

certificate-file *file-name*

undo certificate-file

デフォルト

EAP 認証のためのローカル証明書が指定されていません。

View

EAP profile view

定義済みユーザロール

network-admin

パラメータ

file-name: ローカル証明書ファイル名を指定します。大文字と小文字を区別する 1～91 文字の文字列です。PEM 形式の証明書ファイルのみをサポートします。

説明

certificate-file コマンドは、EAP 認証のためのローカル証明書ファイルを指定します。

undo certificate-file コマンドを使用して、デフォルトの状態を復元します。

PEAP-MSCHAPv2、TTLS-MSCHAPv2 の EAP 認証方式を使用し、RADIUS クライアントが RADIUS サーバの証明書認証を要求する場合は、ローカル証明書ファイルを指定する必要があります。

ローカル証明書ファイルを指定する前に、FTP または TFTP を使用してデフォルトストレージメディアのルートディレクトリにファイルを転送する必要があります。クラウドクラスタの場合は、各メンバーデバイスのデフォルトストレージメディアのルートディレクトリにファイルがすでに存在していることを確認してください。

EAP プロファイルで指定できるローカル証明書ファイルは 1 つだけです。このコマンドを複数回実行した場合は、最新の設定が有効になります。

RADIUS サーバを起動するには、ローカル証明書ファイルを指定する必要があります。

例

EAP プロファイル eap1 で、EAP 認証のローカル証明書ファイルとして証明書ファイル server.pem を指定します。

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] certificate-file server.pem
```

3.4.3 eap-profile

Syntax

eap-profile *eap-profile-name*

undo eap-profile *eap-profile-name*

デフォルト

EAP プロファイルが存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

eap-profile-name: EAP プロファイル名を指定します。1～32 文字の大文字と小文字を区別する文字列です。

説明

eap-profile コマンドは、EAP プロファイルを作成し、そのビューに入るか、既存の EAP プロファイルのビューに入ります。

undo eap-profile コマンドを使用して、EAP プロファイルを削除します。

EAP プロファイルは、EAP 認証方式および認証パラメータを含む、EAP 認証設定の集まりであり、RADIUS サーバが認証を実行する際に使用されます。

最大 16 個の EAP プロファイルを設定できます。

EAP プロファイルがローカル RADIUS サーバに適用されている場合、EAP プロファイル内のすべての設定は、radius-server activate コマンドを使用して RADIUS サーバの設定が有効化された後にのみ反映されます。

例

EAP プロファイル eap1 を作成し、そのビューに入ります。

<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1]

3.4.4 method

Syntax

method { md5 | peap-mschapv2 | ttls-mschapv2 }

undo method

デフォルト

デフォルトの EAP 認証方式は MD5-challenge 方式です。

View

EAP profile view

定義済みユーザロール

network-admin

パラメータ

md5: MD5-challenge 方式を指定します。

peap-mschapv2: PEAP-MSCHAPv2 方式を指定します。

ttls-mschapv2: TTLS-MSCHAPv2 方式を指定します。

🕮 **メモ：**

PEAP-GTC、TTLS-GTC、EAP-TLS での EAP 認証方式はサポートしていません。

説明

method コマンドは、デフォルトの EAP 認証方式を指定します。

undo method コマンドを使用して、デフォルトの状態を復元します。

EAP プロファイルでは、デフォルトの EAP 認証方式は 1 つだけ指定できます。このコマンドを複数回実行した場合、最新の設定が有効になります。

本機器は複数の EAP 認証方式をサポートしています。本機器がピアに対して認証要求を開始する際、EAP プロファイルで設定されたデフォルトの EAP 認証方式が優先的に使用されます。ピアが異なる EAP 認証方式を使用している場合、そのピアがサポートする EAP 認証方式を本機器に通知します。本機器は、ローカルとピアの両方でサポートされている方式を選択し、再度認証要求を開始します。

例

EAP プロファイル eap1 で、デフォルトの EAP 認証方式として PEAP-MSCHAPv2 を指定してください。

<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] method peap-mschapv2

3.4.5 private-key-file

Syntax

private-key-file *file-name*

undo private-key-file

デフォルト

ローカル証明書のプライベートキー ファイルが指定されていません。

View

EAP profile view

定義済みユーザロール

network-admin

パラメータ

file-name:秘密鍵ファイル（1～91 文字の大文字と小文字を区別する文字列）を指定します。PEM 形式の秘密鍵ファイルのみサポートします。

説明

private-key-file コマンドは、ローカル証明書のプライベートキー・ファイルを指定します。

undo private-key-file コマンドを使用して、デフォルトの状態を復元します。

PEAP-MSCHAPv2、TTLS-MSCHAPv2 の EAP 認証方式を使用する場合、RADIUS クライアントによって暗号化された情報を RADIUS サーバが復号するために、秘密鍵ファイルを指定する必要があります。

EAP 認証用のローカル証明書ファイルに秘密鍵が含まれている場合は、秘密鍵ファイルとしてローカル証明書ファイルを指定してください。

秘密鍵ファイルを指定する前に、FTP または TFTP を使用してファイルをデバイスのデフォルトストレージメディアのルートディレクトリに転送する必要があります。クラウドクラスタの場合、各メンバーデバイスのデフォルトストレージメディアのルートディレクトリにファイルが既に存在していることを確認してください。

EAP プロファイルでは、秘密鍵ファイルは 1 つしか指定できません。このコマンドを複数回実行した場合、最新の設定が有効になります。

RADIUS サーバを起動するためには、秘密鍵ファイルを指定する必要があります。

例

EAP プロファイル eap1 で、ローカル証明書用にプライベートキー・ファイル server.pem を指定します。

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] private-key-file server.pem
```

3.4.6 private-key-password

Syntax

private-key-password { **cipher** | **simple** } *string*

undo private-key-password

デフォルト

ローカル証明書の秘密鍵パスワードが指定されていません。

View

EAP profile view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号化された形式でパスワードを指定します。

simple: 平文形式でパスワードを指定します。セキュリティ上の理由から、平文で指定されたパスワードは暗号化された形式で保存されます。

string: パスワードを指定します。暗号化形式では 1～117 文字の大文字と小文字を区別する文字列です。平文形式では 1～63 文字の大文字と小文字を区別する文字列です。

説明

private-key-password コマンドは、ローカル証明書の秘密鍵パスワードを指定します。

undo private-key-password コマンドを使用して、デフォルトの状態を復元します。

デバイスがローカル証明書の秘密鍵をインポートまたは使用する際には、秘密鍵のパスワードを指定する必要があります。このコマンドで指定した秘密鍵のパスワードが、秘密鍵をデバイスにインポートする際に提供したパスワードと同じであることを確認してください。

EAP プロファイルでは、秘密鍵のパスワードを一つだけ指定できます。このコマンドを複数回実行した場合、最新の設定が有効になります。

RADIUS サーバーを起動するためには、秘密鍵のパスワードを指定する必要があります。

例

EAP プロファイル eap1 で、ローカル証明書のプライベートキーパスワードとして平文パスワード 123 を指定します。

```
<Sysname> system-view
[Sysname] eap-profile eap1
[Sysname-eap-profile-eap1] private-key-password simple 123
```

3.5 RADIUSサーバ設定コマンド

🕮 **メモ**:

この機能は、ソフトウェアバージョン 9.6.08c を含む以降のソフトウェアからサポートしています。

3.5.1 display radius-server active-client

Syntax

display radius-server active-client

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display radius-server active-client コマンドを使用して、アクティブな RADIUS クライアントに関する情報を表示します。

例

#アクティブ化されているすべての RADIUS クライアントの情報を表示します。

<Sysname> display radius-server active-client
Total 2 RADIUS clients.
Client IP: 2.2.2.2
Client IP: 3.3.3.3

表 3-8 display radius-server active-client コマンドの表示情報の説明

フィールド	説明
Total 2 RADIUS clients	アクティブ化されたRADIUSクライアントの総数
Client IP	RADIUSクライアントのIPアドレス

3.5.2 display radius-server active-eap-profile

Syntax

display radius-server active-eap-profile

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display radius-server active-eap-profile コマンドを使用して、アクティブ化された EAP プロファイルに関する情報を表示します。

例

#アクティブ化された EAP プロファイルの情報を表示します。

<Sysname> display radius-server active-eap-profile
Method : PEAP-MSCHAPv2
CA file : ca.pem
Certificate file : server.pem
Private key file : server.pem

表 3-9 display radius-server active-client コマンドの表示情報の説明

フィールド	説明
Method	EAP認証方式
CA file	CA証明書ファイル名
Certificate file	ローカル証明書ファイル名
Private key file	秘密鍵ファイルの名

3.5.3 display radius-server active-user

Syntax

display radius-server active-user [*user-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-name: RADIUS ユーザ名を指定します。ドメイン名を含めず、大文字と小文字を区別する 1～55 文字の文字列です。

RADIUS ユーザ名を指定しない場合、有効化されているすべての RADIUS ユーザに関する情報を表示します。

説明

display radius-server active-user コマンドを使用して、アクティブな RADIUS ユーザの情報を表示します。

例

#有効化された RADIUS ユーザー「test」に関する情報を表示します。

```
<Sysname> display radius-server active-user test
Total 1 RADIUS users matched.

Username: test
  Description: A network access user from company cc
  Authorization attributes:
    VLAN ID: 2
    ACL number: 2000
  Validity period:
```

```
    Expiration time: 2020/02/03-18:00:00
# Display information about all activated RADIUS users.
<Sysname> display radius-server active-user
Total 2 RADIUS users matched.

Username: 123
  Description: A network access user from company cc
  Authorization attributes:
    VLAN ID: 2
    ACL number: 3000
  Validity period:
    Expiration time: 2020/02/03-18:00:00

Username: 456
  Description: A network access user from company cc
  Authorization attributes:
    VLAN ID: 2
    ACL number: Not configured
  Validity period:
    Expiration time: Not configured
```

表 3-10 display radius-server active-user コマンドの表示情報の説明

フィールド	説明
Username	RADIUSユーザ名
Description	RADIUSユーザの説明。
Authorization attributes	RADIUSユーザの認可属性
VLAN ID	認可VLAN
ACL number	認可ACL
Validity period	RADIUSユーザの有効期間
Expiration time	RADIUSユーザの有効期限日時

3.5.4 radius-server activate

Syntax

radius-server activate

View

System view

定義済みユーザロール

network-admin

説明

radius-server activate コマンドを使用して、RADIUS サーバプロセスを再起動し、RADIUS サーバの設定を有効にします。

起動時に、デバイスは自動的に RADIUS サーバプロセスを開始し、RADIUS サーバの設定（RADIUS クライアント、RADIUS ユーザ、および EAP プロファイル設定を含む）を有効化します。

以下のいずれかの操作を行った後、RADIUS サーバプロセスを再起動し、最新の RADIUS サーバ設定を有効化するには、このコマンドを使用します。

・RADIUS クライアントまたは RADIUS ユーザの追加、変更、削除を行った場合

・RADIUS サーバに指定された EAP プロファイル設定（EAP プロファイルビューで設定）を変更した場合

RADIUS サーバプロセスが再起動中は、デバイスは RADIUS サーバとして RADIUS ユーザに対する認証サービスを提供できません。

例

RADIUS サーバプロセスを再起動し、RADIUS サーバの設定を有効化してください。

<Sysname> system-view
[Sysname] radius-server activate

3.5.5 radius-server client

Syntax

radius-server client ip *ipv4-address* **key** { **cipher** | **simple** } *string*

undo radius-server client { **all** | **ip** *ipv4-address* }

デフォルト

RADIUS クライアントが指定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*: RADIUS クライアントの IPv4 アドレスを指定します。第 1 オクテットが 0 または 127 を除く、クラス A、B、C のアドレスが指定できます。

key: RADIUS サーバが RADIUS クライアントと通信するために使用する共有キーを指定します。

cipher: 暗号化された形式のキーを指定します。

simple: 平文形式のキーを指定します。

string: 大文字と小文字を区別するキー文字列を指定します。キーの暗号化形式は 1～117 文字の文字列、平文形式は 1～64 文字の文字列です。

all: すべての RADIUS クライアントを指定します。

説明

radius-server client コマンドを使用して、RADIUS クライアントを指定します。

undo radius-server client コマンドを使用して、RADIUS クライアントを削除します。

RADIUS クライアントの IP アドレスは、RADIUS クライアントで指定された送信 RADIUS パケットの送信元 IP アドレスと同じでなければなりません。

RADIUS クライアントの共有キーは、RADIUS クライアント上の設定と同じでなければなりません。

このコマンドは複数回実行することで、複数の RADIUS クライアントを指定できます。

例

IP アドレス 2.2.2.2 のホストを RADIUS クライアントとして指定し、共有キーを平文で test に設定します。

<Sysname> system-view
[Sysname] radius-server client ip 2.2.2.2 key simple test

3.5.6 radius-server deactivate

Syntax

radius-server deactivate

View

System view

定義済みユーザロール

network-admin

説明

radius-server deactivate コマンドを使用して、RADIUS サーバプロセスをシャットダウンし、RADIUS サーバの設定を無効化します。RADIUS サーバプロセスがシャットダウンされると、デバイスは RADIUS サーバとして RADIUS ユーザの認証サービスを提供できなくなります。

例

RADIUS サーバプロセスを終了し、RADIUS サーバの設定を無効化します。

<Sysname> system-view
[Sysname] radius-server deactivate

3.5.7 radius-server eap-profile

Syntax

radius-server eap-profile *eap-profile-name*

undo radius-server eap-profile

デフォルト

RADIUS サーバに指定された EAP プロファイルがありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

eap-profile-name: EAP プロファイル名を指定します。1～32 文字の大文字と小文字を区別する文字列です。作成済の EAP プロファイルを指定する必要があります。

説明

radius-server eap-profile コマンドを使用して、RADIUS サーバの EAP プロファイルを指定します。

undo radius-server eap-profile を使用して、デフォルトの状態を復元します。

起動後、RADIUS サーバは EAP プロファイル内の EAP 認証方式および関連パラメータを使用して、管理された RADIUS クライアントとやり取りします。

EAP プロファイルは、**radius-server activate** コマンドで RADIUS サーバの設定を有効化した後にのみ有効になります。

radius-server eap-profile コマンドを複数回実行した場合、最新の設定が有効になります。

例

RADIUS サーバに対して EAP プロファイル eap1 を指定します。

<Sysname> system-view
[Sysname] radius-server eap-profile eap1

目次

このセクションのページは **13-x-x** です。

4 章 Portal 4-1
4.1 Portal 設定コマンド 4-1
4.1.1 web-redirect url 4-1

4章 Portal

4.1 Portal設定コマンド

4.1.1 web-redirect url

Syntax

web-redirect url *url-string* **[interval** *interval* **]**

undo web-redirect

デフォルト

無効

View

Interface view

Service template view

定義済みユーザロール

network-admin

パラメータ

url *url-string*：ユーザのリダイレクト先の URL を 1 文字から 256 文字の文字列で指定します。URL は存在する URL を指定してください。形式は、http://または https://で始まる完全な URL であることを確認してください。URL 文字列には疑問符 (?) を含めることができます。url-string 引数の場所に疑問符 (?) を入力した場合、CLI はこの引数のヘルプ情報を表示しません。

interval *interval*：指定した URL にユーザがリダイレクトされる時間間隔を指定します。60 秒から 86400 秒の範囲で指定します。デフォルトの間隔は 86400 秒です。

説明

web-redirect url コマンドは Web リダイレクト機能を有効にします。

undo web-redirect url コマンドは Web リダイレクト機能を無効にします。

この機能は、Web ブラウザを介して外部ネットワークにアクセスする前に、ユーザを指定された URL にリダイレクトします。指定された間隔が経過すると、ユーザは再び指定された URL にリダイレクトされます。

Web リダイレクト機能は、デフォルトのポート番号 80 を使用する HTTP パケットでのみ有効です。

デバイス URL を Web リダイレクト URL として使用するか、ユーザがデバイス URL に正常にアクセスできるようにするには、HTTP サービスを有効にする必要があります。HTTP サービスを有効にするには、**ip http enable** コマンドを使用します。

url *url-string* オプションを使用することで、 異なるユーザに異なる広告ページを発信することができます。

設定パラメータは以下の通りです。

・userip=%c:ユーザの IP アドレスです。

・usermac=%m:ユーザの MAC アドレスです。

・nasid=%n:デバイスの NAS 識別子です。

・ssid=%E:ユーザが関連付ける SSID です。

・originalurl=%o:ユーザがブラウザに入力する元の URL です

パラメータ形式は以下の形式に準拠していることを確認してください。

http://XXXX/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o

例

#サービステンプレート service 1 で Web リダイレクトを設定します。リダイレクト URL を http://192.0.0.1/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originall=%o に設定します。間隔は 3600 秒に設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] web-redirect url http://192.0.0.1/index.html?userip=%c&usermac=%m&nasid=%n&ssid=%E&originalurl=%o interval 3600

目次

このセクションのページは **13-x-x** です。

5 章 ポートセキュリティ 5-1
5.1 ポートセキュリティ設定コマンド 5-1
5.1.1 port-security oui 5-1

5章 ポートセキュリティ

5.1 ポートセキュリティ設定コマンド

5.1.1 port-security oui

Syntax

port-security oui index *index-value* **mac-address** *oui-value*

undo port-security oui index *index-value*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

index-value:OUI インデックスを 1 から 16 の範囲で指定します。

oui-value:OUI 文字列、48 ビット MAC アドレスを H-H-H 形式で指定します。システムは、上位 24 ビットのみを OUI 値として使用します。

説明

ユーザ認証の OUI 値を設定するには、**port-security oui** コマンドを使用します。

指定した OUI インデックスを持つ OUI 値を削除するには、**undo port-security oui** コマンドを使用します。

複数の OUI 値を設定できます。

OUI (MAC アドレスの最初の 24 バイナリビット) は、デバイスベンダーを一意に識別するために IEEE によって割り当てられます。特定のベンダーのデバイスが認証されずにネットワークにアクセスできるようにするには、このコマンドを使用します。たとえば、IP 電話とプリンタの OUI を指定できます。

このコマンドで設定された OUI 値は、userLoginWithOUI モードで動作しているポートにのみ適用されます。userLoginWithOUI モードでは、ポートは 1 人の 802.1X ユーザと、設定された OUI 値のいずれかと MAC アドレスが一致する 1 人のユーザだけを許可します。

例

OUI 値 000d2a をセットし、インデックスを 4 に設定します。

<Sysname> system-view

[Sysname] port-security oui index 4 mac-address 000d-2a10-0033

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

14. 高可用性

本マニュアルは以下に示す章で構成されています。

01-WLAN 高可用性

02-Track

03-クラウドクラスタ

目次

このセクションのページは **14-x-x** です。

1 章 WLAN 高可用性 1-1
1.1 デュアルリンクバックアップ設定コマンド 1-1
1.1.1 backup-ac 1-1
1.1.2 wlan tunnel-preempt 1-2
1.2 AP ホットバックアップ 1-3
1.2.1 wlan ap-backup hot-backup enable 1-3
1.3 クライアントホットバックアップ 1-4
1.3.1 display dot1x connection-backup 1-4
1.3.2 display mac-authentication connection-backup 1-7
1.3.3 display wlan client-backup 1-9
1.3.4 wlan client-backup hot-backup 1-16
1.3.5 wlan client-backup hot-backup delay 1-17

1章 WLAN 高可用性

1.1 デュアルリンクバックアップ設定コマンド

1.1.1 backup-ac

Syntax

backup-ac ip *ipv4-address*

undo backup-ac ip

デフォルト

AP view:AP グループ設定を継承します。

AP group view:バックアップ AC の IP アドレスが設定されていません。

View

AP view

AP group view

定義済みユーザロール

network-admin

パラメータ

ip ip-address:バックアップ AC の IPv4 アドレス。

説明

backup-ac コマンドを使用して、デュアルリンクモードでバックアップ AC の IP アドレスを設定します。

undo backup-ac コマンドを使用して、バックアップ AC の IPv4 アドレスまたは IPv6 アドレスを削除します。

AP view では、バックアップ AC の IPv4 アドレスは最大 1 つ、IPv6 アドレスは最大 1 つしか構成できません。

AP group view では、バックアップ AC の IPv4 アドレスは最大 1 つ、IP 6 アドレスは最大 1 つしか設定できません。

AP グループのバックアップ AC アドレスと AP view のバックアップ AC アドレスの両方が設定されている場合は、AP view のバックアップ AC アドレスが優先されます。AP view でバックアップ AC アドレスをクリアした後、AP グループのバックアップ AC アドレスが存在する場合は、AP グループに設定されているバックアップ AC アドレスが使用されます。

バックアップトンネルが確立されている場合、バックアップ AC の IP アドレスを削除すると、バックアップトンネル接続が切断されます。

例

#バックアップ AC の IPv4 アドレスを設定します。(AP view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-wlan-ap-ap1] backup-ac ip 192.168.1.1

#AP グループのバックアップ AC の IPv4 アドレスを設定します。(AP group view)

<Sysname> system-view

[Sysname] wlan ap-group 1

[Sysname-wlan-ap-group-1] backup-ac ip 192.168.1.1

1.1.2 wlan tunnel-preempt

Syntax

wlan tunnel-preempt { disable | enable }

undo wlan tunnel-preempt

デフォルト

AP view:AP グループが設定されている場合、AP グループの設定を継承します。AP グループが設定されていない場合、グローバル設定が継承されます。

AP group view:グローバル設定を継承します。

グローバル構成ビュー:CAPWAP プライマリトンネルのプリエンプト機能が無効になっています。

View

AP view

AP group view

Global configuration view

定義済みユーザロール

network-admin

説明

wlan tunnel-preempt enable コマンドは、CAPWAP のプライマリトンネルプリエンプト機能を有効にします。

wlan tunnel-preempt disable コマンドは、CAPWAP プライマリトンネルプリエンプト機能をオフにします。

undo wlan tunnel-preempt コマンドを使用して、デフォルトの状態を復元します。

デフォルトでは、デュアルリンクバックアップグループネットワーク環境で、AP 接続のプライマリ AC に障害が発生すると、バックアップ AC は CAPWAP バックアップトンネルをプライマリトンネルに変換します。バックアップ AC が CAPWAP プライマリトンネルプリエンプト機能を有効にすると、バックアップ AC で設定された AP 接続 AC の優先順位がプライマリ AC で設定された優先順位よりも高い場合、バックアップ AC は CAPWAP バックアップトンネルをプライマリトンネルに切り替えます。

例

#CAPWAP マスタートンネルプリエンプト機能を有効にします。(AP view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1020

[Sysname-ap-ap1] wlan tunnel-preempt enable

#CAPWAP マスタートンネルプリエンプト機能を有効にします。(AP group view)

<Sysname> system-view

[Sysname] wlan ap-group group1

[Sysname-wlan-ap-group-group1] wlan tunnel-preempt enable

#CAPWAP マスタートンネルプリエンプト機能を有効にします。(グローバル構成ビュー)

<Sysname> system-view

[Sysname] wlan global-configuration

[Sysname-wlan-global-configuration] wlan tunnel-preempt enable

1.2 APホットバックアップ

1.2.1 wlan ap-backup hot-backup enable

Syntax

wlan ap-backup hot-backup enable

undo wlan ap-backup hot-backup enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

AP ホットバックアップを有効にするには、**wlan ap-backup hot-backup enable** を使用します。

AP ホットバックアップを無効にするには、**undo wlan ap-backup hot-backup enable** を使用します。

AP ホットバックアップを有効にすると、アクティブ AC は、接続されているすべての AP に関する情報をクラウドクラスタ内の他の AC にバックアップします。アクティブ AC に障害が発生すると、システムは自動的にプライマリ AC を新しいアクティブ AC として選択し、障害が発生した AC に接続されている AP を回復します。これにより、AP がオンラインのままであることが保証されます。

この機能は、この機能が有効になった後に、クラウドクラスタに接続された AP に関する情報のみをバックアップします。

この機能を無効にすると、すべての AC でバックアップ AP 情報が削除されます。

例

#AP ホットバックアップを有効にします。

<Sysname> system-view

[Sysname] wlan ap-backup hot-backup enable

1.3 クライアントホットバックアップ

1.3.1 display dot1x connection-backup

Syntax

display dot1x connection-backup [**ap** *ap-name* [**radio** *radio-id*]] **slot** *slot-number*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*:AP を名前で指定します。大文字と小文字が区別され、1 から 64 文字の文字列で指定します。文字、数字、アンダースコア(_)、ドット（。）、左括弧（[）、右括弧(])、スラッシュ(/)、ハイフン(-)のみ使用できます。このオプションを指定しない場合、すべての AP から収集された情報が表示されます。

radio *radio-id*:無線を ID で指定します。無線 ID の範囲は AP の機種によって異なります。このオプションを指定しない場合、すべての無線から収集された情報が表示されます。

slot *slot-number*:クラウドクラスタ内のメンバ ID でメンバデバイスを指定します。

説明

display dot1x connection-backup を使用して、AC の 802.1 X 認証ユーザに関するバックアップ情報を表示します。

例

#AC の 802.1 X 認証ユーザに関するバックアップ情報を表示します。

<Sysname> display dot1x connection-backup ap ap1 slot 1

```
Total backup connections: 1

User MAC address            : 0015-e9a6-7cfe
AP name                    : ap1
Radio ID                   : 1
SSID                       : EASY
BSSID                      : 0015-e9a6-7cf0
Username                   :  ias
IPv4 address               :  192.168.1.1
IPv6 address               :  2000:0:0:0:1:2345:6789:abcd
Authentication method       :  CHAP
Authentication domain       : 1
Initial VLAN               : 1
Authorization VLAN          : 100
Authorization ACL number     : 3001
Authorization user profile   : N/A
Authorization CAR           :
  Average input rate        : 102400 bps
  Average output rate       : 102400 bps
Authorization URL           : N/A
Termination action          : Radius-request
Session timeout period       : 2 sec
Online from                : 2017/03/02 13:14:15
Online duration             : 0h 2m 15s
```

表 1-1 コマンド出力

フィールド	説明
Total backup connections	バックアップ802.1 X認証ユーザの数。
IPv4 address	ユーザのIPv 4アドレス。 システムがユーザのIPv 4アドレスの取得に失敗した場合、 このフィールドは表示されません。

フィールド	説明
IPv6 address	ユーザのIPv 6アドレス。 システムがユーザのIPv 6アドレスの取得に失敗した場合、このフィールドは表示されません。
Authentication method	802.1 X認証方式: • CHAP:CHAP認証によるEAP termination。 • EAP:すべてのEAP認証方式がサポートされているEAP relay。 • PAP:PAP認証によるEAP termination。
Authentication domain	認証に使用されるISP ドメイン。
Authorization CAR	ユーザに認可CAR属性がない場合、このフィールドにはN/Aが表示されます。 認可CAR: • Average input rate:平均アップリンクレート（bps単位）。 • Average output rate:平均ダウンリンクレート（bps単位）。
Authorization URL	ユーザに許可されたリダイレクトURL。
Termination action	サーバによって発行された終了アクション: • **Default:**セッションがタイムアウトした後、ユーザを強制的にオフラインにします。定期的な再認証が有効で、再認証タイマー値がセッションタイムアウトよりも短い場合、ユーザアクセスインタフェースは、ユーザを強制的にオフラインにするのではなく、再認証タイマー値の間隔で再認証を開始します。 • **Radius-Request:**セッションがタイムアウトしたときに、802.1 Xユーザに再認証の実行を要求します。 ローカル認証が使用されている場合、このフィールドには**N/A**が表示されます。
Session timeout period	サーバによって発行されたセッションタイムアウト。セッションがタイムアウトした後、ユーザに対して実行するアクションは、**Terminate action**フィールドによって決定されます。 ローカル認証が使用されている場合、このフィールドには**N/A**が表示されます。
Online from	802.1 X認証ユーザがオンラインになった時刻。
Online duration	802.1 X認証ユーザのオンライン期間。

1.3.2 display mac-authentication connection-backup

Syntax

display mac-authentication connection-backup [**ap** *ap-name* [**radio** *radio-id*]] **slot** *slot-number*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*:AP を名前で指定します。大文字と小文字が区別され、1 から 64 文字の文字列で指定します。文字、数字、アンダースコア(_)、ドット（。）、左括弧（[）、右括弧(])、スラッシュ(/)、ハイフン(-)のみ使用できます。このオプションを指定しない場合、すべての AP から収集された情報が表示されます。

radio *radio-id*:無線を ID で指定します。無線 ID の範囲は AP の機種によって異なります。このオプションを指定しない場合、すべての無線から収集された情報が表示されます。

slot *slot-number*:クラウドクラスタ内のメンバ ID でメンバデバイスを指定します。

説明

AC の MAC 認証ユーザのバックアップ情報を表示するには、**display mac-authentication connection-backup** を使用します。

例

#AP ap 1 に関連付けられた MAC 認証ユーザのバックアップ情報を表示します。

<Sysname> display mac-authentication connection-backup ap ap1 slot 1

```
Total backup connections: 1

User MAC address            : 0015-e9a6-7cfe
AP name                    : ap1
Radio ID                   : 1
SSID                       : EASY
BSSID                      : 0015-e9a6-7cf0
Username                   : ias
Authentication domain        : 1
Authentication method        : PAP
Initial VLAN               : 1
Authorization VLAN          : 100
Authorization ACL number     : 3001
```

```
Authorization user profile    : N/A
Authorization CAR           :
  Average input rate         : 102400 bps
  Average output rate        : 102400 bps
Authorization URL           : N/A
Termination action          : Radius-request
Session timeout period       : 2 sec
Online from                : 2017/03/02 13:14:15
Online duration             : 0h 2m 15s
```

表 1-2 コマンド出力

フィールド	説明
Total backup connections	バックアップMAC認証ユーザの数。
Authentication domain	認証に使用されるIPSドメイン。
Authorization CAR	ユーザに認可CAR属性がない場合、このフィールドには**N/A**が表示されます。 認可CAR: • **Average input rate:**平均アップリンクレート (bps単位) 。 • **Average output rate:**平均ダウンリンクレート (bps単位) 。
Authorization URL	ユーザに認可されたリダイレクトURL。
Termination action	サーバが発行した終了アクション: • **Default:**セッションがタイムアウトした後、ユーザを強制的にオフラインにします。 • **Radius-Request:**セッションがタイムアウトしたときに、MAC認証ユーザに再認証の実行を要求します。 ローカル認証が使用されている場合、このフィールドには**N/A**と表示されます。
Session timeout period	サーバによって発行されたセッションタイムアウト。セッションがタイムアウトした後、ユーザに対して実行するアクションは、**Terminate action**フィールドによって決定されます。 ローカル認証が使用されている場合、このフィールドには**N/A**が表示されます。
Online from	MAC認証ユーザがオンラインになった時刻。
Online duration	MAC認証ユーザのオンライン期間。

1.3.3 display wlan client-backup

Syntax

display wlan client-backup [**ap** *ap-name* [**radio** *radio-id*] | **mac-address** *mac-address*] [**verbose**] [**slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ap *ap-name*:AP を名前で指定します。大文字と小文字が区別され、1 から 64 文字の文字列で指定します。文字、数字、アンダースコア(_)、ドット（。）、左括弧（[）、右括弧(()]）、スラッシュ(/)、ハイフン(-)のみ使用できます。このオプションを指定しない場合、すべての AP から収集された情報が表示されます。

radio *radio-id*:無線を ID で指定します。無線 ID の範囲は AP の機種によって異なります。このオプションを指定しない場合、すべての無線から収集された情報が表示されます。

mac-address *mac-address*:クライアントを MAC アドレスで指定します。

verbose:詳細情報を表示します。このキーワードを指定しない場合、コマンドは簡単な情報を表示します。

slot *slot-number*:クラウドクラスタ内のメンバ ID でメンバデバイスを指定します。プライマリ AC は、クライアントのホットバックアップ情報を保存しません。クライアントのホットバックアップ情報を表示するには、セカンダリ AC を指定します。

説明

クラウドクラスタ内の指定したメンバデバイスのクライアントホットバックアップ情報を表示するには、**display wlan client-backup** を使用します。

ap キーワードと **radio** キーワードを指定しない場合、すべての AP とすべての無線から収集されたクライアントホットバックアップ情報が表示されます。

例

#スロット 2 の簡単なクライアントのホットバックアップ情報を表示します。

<Sysname> display wlan client-backup slot 2

```
Total number of clients: 3
```

```
MAC address     Username   AP name         RID  IP address      IPv6 address
VLAN
7854-2e1c-c59e  user       ap1            1    1.1.1.1         1::2:0:0:3     1
000b-c002-9d09  N/A        5866-ba74-e780 1    192.168.33.16                  200
000f-e265-6400  N/A        ap2            1    1.3.1.2                     100
```

表 1-3 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス。
Username	クライアントのユーザ名。802.1 X/MAC認証ユーザの場合、このフィールドにはユーザ名が表示されます。 非802.1 X/非MAC認証ユーザの場合、このフィールドには**N/A**が表示されます。 ポータル認証が使用されている場合、このフィールドにはポータルユーザ名は表示されません。
AP name	クライアントに関連付けられたAPのID。
RID	クライアントに関連付けられた無線のID。
IP address	クライアントのIPv 4アドレス。
IPv6 address	クライアントのIPv 6アドレス。
VLAN	クライアントVLAN。

#スロット 2 の詳細なクライアントホットバックアップ情報を表示します。

<Sysname> display wlan client-backup slot 2 verbose

```
Total number of clients: 1

MAC address                    : 000f-e265-6400
IPv4 address                   : 10.1.1.114
IPv6 address                   : 2001::1234:5678:0102:0304
Username                       : N/A
AID                            : 1
AP ID                          : 1
AP name                        : ap1
Radio ID                       : 1
SSID                           : office
BSSID                          : 0026-3e08-1150
VLAN ID                        : 3
```

```
Sleep count                    : 1
Power save mode                : Active
Wireless mode                  : 802.11ac
Channel bandwidth              : 80MHz
SM power save                  : Enabled
SM power save mode             : Dynamic
Short GI for 20MHz             : Supported
Short GI for 40MHz             : Supported
Short GI for 80MHz             : Supported
Short GI for 160/80+80MHz      : Not supported
STBC RX capability             : Not supported
STBC TX capability             : Not supported
LDPC RX capability             : Not supported
SU beamformee capability       : Not supported
MU beamformee capability       : Not supported
Beamformee STS capability      : N/A
Block Ack                      : TID 0 In
Supported VHT-MCS set          : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8
                                 NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8
Supported HT MCS set           : 0, 1, 2, 3, 4, 5, 6, 7,
                                 8, 9, 10, 11, 12, 13, 14,
                                 15, 16, 17, 18, 19, 20,
                                 21, 22, 23
Supported rates                : 6, 9, 12, 18, 24, 36,
                                 48, 54 Mbps
QoS mode                       : WMM
Listen interval                : 10
RSSI                           : 62
Rx/Tx rate                     : 130/11 Mbps
Authentication method          : Open system
Security mode                  : PRE-RSNA
AKM mode                       : Not configured
Cipher suite                   : N/A
User authentication mode       : Bypass
Authorization ACL ID           : 3001(Not effective)
Authorization user profile     : N/A
Roam status                    : N/A
Key derivation                 : SHA1
PMF status                     : Enabled
Forward policy                 : Not configured
Online time                    : 0 days 0 hours 1 minutes 13 seconds
FT status                      : Inactive
```

表 1-4 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス。
IPv4 address	クライアントのIPv 4アドレス。アドレスが存在しない場合、このフィールドにはN/Aと表示されます。
IPv6 address	クライアントのIPv 6アドレス。アドレスが存在しない場合、このフィールドにはN/Aと表示されます。
Username	クライアントのユーザ名。802.1 X/MAC認証ユーザの場合、このフィールドにはユーザ名が表示されます。非802.1 X/非MAC認証ユーザの場合、このフィールドには**N/A**が表示されます。 ポータル認証が使用されている場合、このフィールドにはポータルユーザ名は表示されません。
AID	クライアントアソシエーションID。
AP ID	クライアントに関連付けられたAPのID。
AP name	クライアントに関連付けられたAPの名前。
Radio ID	クライアントに関連付けられた無線のID。
SSID	クライアントに関連付けられたSSID。
VLAN ID	クライアントVLAN。
Sleep count	クライアントがスリープモードに入った回数。
Power save mode	クライアント省電力モード: • **Active:**クライアントはアクティブです。 • **Sleep:**クライアントはスリープモードです。
Wireless mode	クライアント動作モード: • 802.11a. • 802.11b. • 802.11g. • 802.11gn. • 802.11an. • 802.11ac.

フィールド	説明
Channel bandwidth	クライアントチャネル帯域幅: • 20MHz. • 40MHz. • 80MHz. • 160MHz.
SM power save	省電力モードの有効化状態: • **Enabled:**省電力モードを有効にすると、クライアント上の1つのアンテナだけがアクティブになります。他のアンテナはスリープモードです。 • **Disabled**
SM power save mode	SM省電力の有効化モード: • **Dynamic** • **Static**
Short GI for 20MHz	20 MHz帯域幅モードでのショートGIのクライアントサポート: • **Supported.** • **Not supported.**
Short GI for 40MHz	40 MHz帯域幅モードでのショートGIのクライアントサポート: • **Supported.** • **Not supported.**
Short GI for 80MHz	80 MHz帯域幅モードでのショートGIのクライアントサポート: • **Supported.** • **Not supported.**
Short GI for 160/80+80MHz	160/80+80 MHz帯域幅モードでのショートGIのクライアントサポート: • **Supported.** • **Not supported.**
STBC RX capability	クライアントSTBCの受信機能: • **Supported.** • **Not supported.**
STBC Tx capability	クライアントSTBC送信機能: • **Supported.** • **Not supported.**

フィールド	説明
LDPC Rx capability	クライアントLDPC受信機能: • **Supported.** • **Not supported.**
SU beamformee capability	クライアントのシングルユーザのビームフォーミー機能: • **Supported.** • **Not supported.**
MU beamformee capability	クライアントのマルチユーザビームフォーミー機能: • **Supported.** • **Not supported.**
Beamformee STS capability	クライアントbeamformee STS機能。 クライアントがbeamformee STSをサポートしていない場合、このフィールドには**N/A**と表示されます。
Block Ack	QoS TIDのブロック確認ネゴシエーション結果: • **TID 0 In:** リンクデータパケットはBlock Ackをサポートします。 • **TID 0 Out:** リンクデータパケットはBlock Ackをサポートします。 • **TID 0 Both:**アップリンクデータパケットとダウンリンクデータパケットの両方がBlock Ackをサポートします。 • **N/A:**アップリンクデータパケットもダウンリンクデータパケットもBlock Ackをサポートしていません。
Supported VHT-MCS set	クライアントによってサポートされるVHT-MCSセット。
Supported HT MCS set	クライアントによってサポートされるHT MCSセット。
Supported rates	クライアントによってサポートされるレート (Mbps単位) 。
QoS mode	QoSモード: • **N/A:**WMMはサポートされていません。 • **WMM:**WMMはサポートされています。 クライアントはAPとWMMサポートをネゴシエートします。APとクライアントの両方がWMMをサポートする場合にのみ、ネゴシエート結果はWMMサポートになります。
Listen interval	スリープモードのクライアントが、APにバッファされたデータフレームを受信するためにウェイクアップする間隔。単位はビーコン送信間隔。
RSSI	APによって検出されたクライアント信号強度。

フィールド	説明
Rx/Tx rate	クライアントのパケット送受信レート (Mbps単位) 。このレートは、データ、管理、および制御パケットに適用されます。
Authentication method	リンクレイヤ認証方式: • Open system. • Shared key.
Security mode	セキュリティモード: • **RSN:**RSN IEをビーコンフレームおよびプローブ応答で伝送します。 • **WPA:**WPA IEをビーコンフレームおよびプローブ応答で伝送します。 • **PRE-RSN:**RSN IEまたはWPA IEをビーコンフレームおよびプローブ応答で伝送しません。
AKM mode	認証およびキー管理モード: • 802.1X. • PSK. • Not configured
Cipher suite	暗号スイート: • **N/A**—暗号化なし • **WEP40**. • **WEP104**. • **WEP128**. • **CCMP**—AES-CCMP. • **TKIP**.
User authentication mode	ユーザ認証モード: • **Bypass**—ユーザ認証なし • **MAC**. • **802.1X**. • **OUI**.
Authorization ACL number	認可ACL番号。 • 認可ACLが有効な場合、このフィールドにはACL番号が表示されます。 • 許可ACLが有効にならない場合、このフィールドにはACL番号と**Not effective**文字列がサフィックスとして表示されます。 • 許可ACLが存在しない場合、このフィールドには**N/A**と表示されます。

フィールド	説明
Authorization user profile	許可ユーザプロファイル名。 ● 許可ユーザプロファイルが有効な場合、このフィールドにはユーザプロファイル名が表示されます。 ● 許可ユーザプロファイルが有効でない場合、このフィールドにはユーザプロファイル名と**Not effective**文字列がサフィックスとして表示されます。 ● 許可ユーザプロファイルが存在しない場合、このフィールドには**N/A**と表示されます。
Roam status	ローミングステータス: ● oaming in progress. ● Inter-AC roam. ● Inter-MA roam. ● Intra-AC roam. ● Intra-MA roam. ● N/A.
Key derivation	キーの派生アルゴリズム: ● **SHA1**. ● **SHA256**. ● **N/A**—アルゴリズムを使用しません。
PMF status	管理フレーム保護ステータス: ● **Enabled**. ● **Disabled**. ● **N/A**—管理フレームの保護は行いません。
Forward policy	ワイヤレス転送ポリシー名。 ワイヤレス転送ポリシーが設定されていない場合、このフィールドには **Not configured**と表示されます。
Online time	クライアントのオンライン時間。
FT status	FTステータス: ● **Active:**有効。 ● **Inactive:**無効。

1.3.4 wlan client-backup hot-backup

Syntax

wlan client-backup hot-backup enable

undo wlan client-backup hot-backup enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

クライアントのホットバックアップを有効にするには、**wlan client-backup hot-backup enable** を使用します。

クライアントのホットバックアップを無効にするには、**undo wlan client-backup hot-backup enable** を使用します。

クライアントのホットバックアップを有効にするには、AP ホットバックアップも有効にする必要があります。

AP ホットバックアップとクライアントホットバックアップを有効にすると、プライマリ AC は接続されているすべての AP とクライアントに関する情報をクラウドクラスタ内のセカンダリ AC にバックアップします。プライマリ AC で障害が発生すると、セカンダリ AC は障害の発生した AC の AP とクライアントの情報を回復し、クライアントがオンライン状態を維持できるようにします。

システムは、クライアントのホットバックアップが有効になった後にオンラインになったクライアントのデータのみバックアップします。クライアントのホットバックアップを無効にすると、システムはすべての AC のバックアップクライアント情報を削除します。

例

#クライアントのホットバックアップを有効にします。

<Sysname> system-view

[Sysname] wlan client-backup hot-backup enable

1.3.5 wlan client-backup hot-backup delay

Syntax

wlan client-backup hot-backup delay *delay-time*

undo wlan client-backup hot-backup delay

デフォルト

60 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

delay-time:遅延時間を 0 秒から 300 秒の範囲で指定します。値を 0 に設定すると、システムはクライアント情報をリアルタイムでバックアップできます。

説明

クライアントホットバックアップの遅延時間を設定するには、**wlan client-backup hot-backup delay** を使用します。

デフォルトに戻すには、**undo wlan client-backup hot-backup delay** を使用します。

この機能は、クライアントバックアップが有効の場合にのみ有効です。

クライアントバックアップ遅延は、本コマンドの設定後にオンラインになったクライアントにのみ有効です。

遅延時間中にアクティブ/スタンバイスイッチの切り替えが発生した場合、情報がバックアップされていないオンラインクライアントはログオフされ、再度オンラインになる必要があります。アクティブ/スタンバイスイッチの切り替えは、アクティブ AC プロセスの再起動によって開始されます。

例

#クライアントホットバックアップの遅延時間を 240 秒に設定します。

<System> system-view

[System] wlan client-backup hot-backup delay 240

関連コマンド

- wlan client-backup hot-backup enable

目次

このセクションのページは **14-x-x** です。

2 章 Track 2-1
2.1 Track 設定コマンド 2-1
2.1.1 display track 2-1
2.1.2 track interface 2-4
2.1.3 track interface protocol 2-6
2.1.4 track nqa 2-7

2章 Track

2.1 Track設定コマンド

2.1.1 display track

Syntax

display track { *track-entry-number* | **all** [**negative** | **positive**] } [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

all: すべての track エントリの情報を表示します。

negative: Negative 状態のトラックエントリを指定します。

positive: Positive 状態のトラックエントリを指定します。

brief: トラックエントリに関する概要情報を表示します。

説明

display track コマンドは track エントリの情報を表示します。

例

すべての track エントリの情報を表示します。

<System> display track all

```
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 10
    Remote IP/URL: --
    Local IP: --
    Interface: --
```

```
Track ID: 2
  State: NotReady
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    BFD session mode: Echo
    Outgoing interface: Vlan-interface2
    VPN instance name: --
    Remote IP: 192.168.40.1
    Local IP: 192.168.40.2
Track ID: 3
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    Interface:  Vlan-interface3
    Protocol: IPv4
Track ID: 4
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    CFD service instance: MEP 2 in Ethernet service instance 1
Track ID: 5
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    IP route: 0.0.0.0/0 reachability
    VPN instance name: --
    Protocol: BGP
    Nexthop interface : Vlan-Interface4
```

Negative 状態のトラックエントリに関する情報を表示します。

<System> display track all negative brief

```
ID   Status   Type      Remote IP/URL   Local IP       Interface
1    Negative Interface --            --             Vlan2
10   Negative Interface --            --             Vlan3
```

表 2-1 コマンド出力

フィールド	説明
Track ID	trackエントリのIDです。

フィールド	説明
State	trackエントリの状態です。 ● **Positive**—正常にtrackオブジェクトが動作しています。 ● **NotReady**—trackオブジェクトが無効です。 ● **Negative**—trackオブジェクトが異常です。
Duration	trackエントリが状態を保持する時間間隔です。
Notification delay: Positive 20, Negative 30 (in seconds)	● trackモジュールは、trackエントリ状態が20秒の遅延時間後、Positiveに変更するとアプリケーションモジュールに通知します。 ● trackモジュールは、trackエントリ状態が30秒の遅延時間後、Negativeに変更するとアプリケーションモジュールに通知します。
Tracked object	trackエントリに関連づけられたtrackオブジェクトです。
NQA entry	trackエントリに関連づけられたNQAオペレーションです。
Reaction	trackエントリに関連づけられたリアクションエントリです。
BFD session mode	BFDセッションモードです。エコーモードのみサポートします。
Outgoing interface	BFDエコーモードパケットの送信インタフェースです。
VPN instance name	BFDセッションパケットが属しているVPNインスタンス名です。パケットがパブリックネットワークに属している場合、2つの連続したハイフン（--）が表示されます。
Remote IP/URL	リモートIPアドレスまたはURLリモートIPアドレスまたはURLが存在しない場合は、2つの連続したハイフン（--）が表示されます。
Local IP	ローカルIPアドレス。ローカルIPアドレスが存在しない場合は、2つの連続したハイフン（--）が表示されます。
Interface	モニタされるインタフェースです。インタフェースをモニタしない場合は、2つの連続したハイフン(--)が表示されます。
Protocol	モニタされるインタフェースのリンク状態あるいはレイヤ3プロトコルの状態です。 ● **None**—モニタされるインタフェースのリンク状態です。 ● **IPv4**—モニタされるレイヤ3インタフェースのIPv4プロトコルの状態です。 ●
IP route	トラックエントリに関連付けられたルートです。

フィールド	説明
VPN instance name	ルートが属するVPNインスタンスの名前です。ルートがパブリックネットワークに属している場合は、2つの連続したハイフン(--)が表示されます。
Protocol	ルートのプロトコルタイプです。ルートが存在しない場合は、**N/A**と表示されます。
Nexthop interface	ルートのネクストホップです。ルートが存在しない場合は、**N/A**と表示されます。
LLDP interface	モニタされるLLDP インタフェースです。
Type	モニタされるオブジェクトのタイプです。 • BFD • CFD • Interface • LLDP • NQA • Route

関連コマンド

- **track interface**
- **track interface protocol**

2.1.2 track interface

Syntax

track *track-entry-number* **interface** *interface-type interface-number* [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

delay: トラックモジュールは、トラックエントリのステータスの変化を、指定した遅延時間後に、アプリケーションモジュールに通知します。指定しない場合、トラックモジュールは、トラックエントリのステータスが変化すると、すぐにアプリケーションモジュールに通知します。

negative *negative-time*: トラックエントリの状態が Negative に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

positive *positive-time*: トラックエントリの状態が Positive に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

説明

track interface コマンドは track エントリを作成し、インタフェースのリンク状態に関連づけます。

undo track コマンドは track エントリを削除します。

トラックをインタフェース管理に関連付けてインタフェースのリンク状態をモニタすると、トラックのエントリ状態が次のように変化します。

- インタフェースのリンク状態が up である場合、track エントリの状態は Positive です。
- インタフェースのリンク状態が down である場合、track エントリの状態は Negative です。

インタフェースのリンク状態を表示する場合、**display ip interface brief** コマンドを使用します。

track エントリを作成したのち、遅延時間の設定を修正する場合、**track interface delay** コマンドのみを使用することができます。**track interface delay** コマンドを複数回実行すると、最新の設定が有効になります。

track エントリの他の設定を変更するには、**undo track** コマンドを実行して track エントリを削除してから、再度 **track interface** コマンドを実行します。

例

track エントリ 1 を作成し、VLAN インタフェース 10 のリンク状態に関連づけます。

<System> system-view

[System] track 1 interface vlan-interface 10

関連コマンド

- **display track**
- **display ip interface brief** (ネットワーク接続/IP アドレス)

2.1.3 track interface protocol

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol ipv4** [**delay** { **negative** *negative-time* | **positive** *positive-time* } *]

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

ipv4: IPv4 プロトコル状態をモニタします。インタフェースの IPv4 プロトコル状態が up である場合、track エントリの状態は Positive です。インタフェースの IPv4 プロトコル状態が down である場合、track エントリの状態は Negative です。インタフェースの IPv4 プロトコル状態を表示する場合、**display ip interface brief** コマンドを使用します。

delay: トラックモジュールは、トラックエントリのステータスの変化を、指定した遅延時間後に、アプリケーションモジュールに通知します。指定しない場合、トラックモジュールは、トラックエントリのステータスが変化すると、すぐにアプリケーションモジュールに通知します。

negative *negative-time*: トラックエントリの状態が Negative に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

positive *positive-time*: トラックエントリの状態が Positive に変化したことをアプリケーションモジュールに通知するときの遅延時間を指定します。設定範囲は 1～300 秒です。

説明

track interface protocol コマンドは track エントリを作成し、インタフェースのプロトコル状態に関連づけます。

undo track コマンドは track エントリを削除します。

track エントリを作成したのち、遅延時間の設定を修正する場合、**track interface protocol delay** コマンドのみを使用することができます。**track interface protocol delay** コマンドを複数回実行すると、最新の設定が有効になります。

track エントリの他の設定を変更するには、**undo track** コマンドを実行して track エントリを削除してから、再度 **track interface protocol** コマンドを実行します。

例

track エントリ 1 を作成し、VLAN インタフェース 2 の IPv4 プロトコル状態に関連づけます。

<System> system-view

[System] track 1 interface vlan-interface 2 protocol ipv4

関連コマンド

- **display track**
- **display ip interface brief** (ネットワーク接続/IP アドレス)

2.1.4 track nqa

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

entry *admin-name operation-tag*: track エントリに関連づけられる NQA オペレーションを指定します。*admin-name* は NQA オペレーションを作成する NQA オペレーションの管理者名です。設定範囲は 1～32 文字です。大文字、小文字を区別しません。*operation-tag* は NQA オペレーションのタグです。設定範囲は 1～32 文字です。大文字、小文字を区別しません。

reaction *item-number*: track エントリに関連づけられるリアクションエントリを指定します。*item-number* はリアクションエントリの ID です。設定範囲は 1～10 です。

説明

track nqa コマンドを使用して、トラックエントリを作成し、NQA 操作のリアクションを監視し、track entry view に移行するか、既存の track entry view に移行します。

undo track コマンドを使用して、トラックエントリとすべての設定をビューから削除します。

トラックエントリを作成するには、このコマンドの nqa であるトラックオブジェクトタイプを指定する必要があります。

既存のトラックエントリのビューに入るには、**track** *track-entry-number* コマンドを使用します。トラックオブジェクトタイプは必須ではありません。

トラックエントリの設定を変更するには、**undo track** コマンドを実行してトラックエントリを削除し、**track nqa** コマンドを再度実行します。

例

トラックエントリ 1 を作成して、NQA テスト admin-test のリアクションエントリ 3 を監視し、track entry view に移行します。

<AC> system-view

[AC] track 1 nqa entry admin test reaction 3

[AC-track-1]

関連コマンド

- **display track**

目次

このセクションのページは **14-x-x** です。

3 章 クラウドクラスタ 3-1
3.1 クラウドクラスタ 3-1
3.1.1 cloud-cluster auto-merge enable 3-1
3.1.2 cloud-cluster auto-update enable 3-2
3.1.3 cloud-cluster configuration active 3-3
3.1.4 cloud-cluster enable 3-4
3.1.5 cloud-cluster link-delay 3-5
3.1.6 cloud-cluster member 3-6
3.1.7 cloud-cluster member renumber 3-7
3.1.8 cloud-cluster service-cluster domain 3-8
3.1.9 cloud-cluster service-cluster mac-address persistent 3-10
3.1.10 cloud-cluster service-cluster mad domain 3-11
3.1.11 cloudcluster-optimize wlan reliable-access 3-13
3.1.12 cluster-link bind interface 3-13
3.1.13 display cloud-cluster 3-16
3.1.14 display cloud-cluster configuration 3-19
3.1.15 display cloud-cluster service-cluster container 3-21
3.1.16 display mad 3-24
3.1.17 join-cluster 3-26
3.1.18 mad enable 3-28
3.1.19 mad exclude interface 3-29
3.1.20 mad restore 3-31
3.1.21 member-ip 3-31

3章 クラウドクラスタ

3.1 クラウドクラスタ

3.1.1 cloud-cluster auto-merge enable

Syntax

cloud-cluster auto-merge enable

undo cloud-cluster auto-merge enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

クラウドクラスタの自動マージを有効にするには、**cloud-cluster auto-merge enable** を使用します。

クラウドクラスタの自動マージを無効にするには、**undo cloud-cluster auto-merge enable** を使用します。

I. アプリケーションシナリオ

クラウドクラスタの自動マージは、次のイベントによって発生するマージに対して有効になります。

- クラウドクラスタリンクは、リンク障害から回復します。
- マージするクラウドクラスタに既にクラスタリンクの割り当て設定があり、割り当てられたインタフェースが既に接続されている場合は、クラスタリンクをリンクアップにします。

II. 動作メカニズム

クラウドクラスタの自動マージ機能が無効になっている場合は、システムの指示に従って、マスタの選択に失敗したクラウドクラスタ内のメンバデバイスを手動で再起動する必要があります。

クラウドクラスタの自動マージ機能が有効になっている場合は、マスタの選択に失敗したクラウドクラスタ内のメンバデバイスが自動的に再起動して、クラウドクラスタのマージが完了します。

マージを成功させるには、マージするクラウドクラスタでクラウドクラスタの自動マージが有効になっていることを確認します。

例

クラウドクラスタの自動マージ機能を有効にします。

<Sysname> system-view

[Sysname] cloud-cluster auto-merge enable

3.1.2 cloud-cluster auto-update enable

Syntax

cloud-cluster auto-update enable

undo cloud-cluster auto-update enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

ソフトウェアの自動更新を有効にするには、**cloud-cluster auto-update enable** を使用します。

ソフトウェアの自動更新を無効にするには、**undo cloud-cluster auto-update enable** を使用します。

I. 動作メカニズム

ソフトウェア自動更新機能は、クラウドクラスタに参加しようとしているデバイスにマスタの現在のソフトウェアイメージを自動的に同期します。

ソフトウェア自動更新が無効になっていて、クラスタに参加しようとしている新しいデバイスのソフトウェアイメージが Master と異なる場合は、ソフトウェアの不整合によって新しいデバイスはクラスタに参加できません。ソフトウェアの自動更新を有効にして、すべてのデバイスで同じソフトウェアを使用することを推奨します。

II. 前提条件

クラスタに追加するデバイスに、新しいソフトウェアイメージ用の十分なストレージ領域があることを確認します。

十分なストレージ領域がない場合、デバイスは現在のソフトウェアイメージを自動的に削除します。領域がまだ不足している場合、デバイスは自動更新を完了できません。デバイスを再起動し、Boot メニューにアクセスしてファイルを削除する必要があります。

例

ソフトウェア自動更新機能を有効にします。

<Sysname> system-view

[Sysname] cloud-cluster auto-update enable

3.1.3 cloud-cluster configuration active

Syntax

cloud-cluster configuration active

View

System view

定義済みユーザロール

network-admin

説明

クラウドクラスタ設定を有効化にするには、**cloud-cluster configuration active** を使用します。

I. アプリケーションのシナリオ

クラウドクラスタ設定を編集した後、新しい構成を有効にするには、このコマンドを実行して設定を有効化する必要があります。

II. 推奨されるアクション

1) クラウドクラスタの設計計画を行います。
2) 事前にすべてのメンバデバイスの設定(メンバ ID、メンバ IP、クラスタ IP、クラウドクラスタリンクの物理インタフェースなど)を設定します。
3) 指定したクラスタリンクにケーブルを接続します。
4) このコマンドを実行してクラスタを構築します。

III. 制限とガイドライン

このコマンドの実行後にデバイスが自動的に再起動するかどうかについては、デバイスのプロンプト情報を参照してください。

例

#クラスタのメンバデバイス設定を行った後、設定を有効にします。

<Sysname> system-view

[Sysname] cloud-cluster member 1 renumber 2

[Sysname] cloud-cluster configuration active

```
New cluster configuration:
  cloud-cluster service-cluster domain 0
  cloud-cluster hello cloud-timeout 7 service-timeout 10
  cloud-cluster member 2
    role manager-worker
    cluster-link bind interface GigabitEthernet 2/0/2
    cluster-link bind interface GigabitEthernet 2/0/3
The system will activate and save the configuration, and it might do a restart.
Continue? [Y/N]: y
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter
key):flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully
```

関連コマンド

- cloud-cluster member remember
- cloud-cluster service-cluster domain
- cluster-link bind interface
- ip address
- join cluster

3.1.4 cloud-cluster enable

Syntax

cloud-cluster enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

本コマンドは常に有効です。

クラウドクラスタ機能の無効化はできません。

3.1.5 cloud-cluster link-delay

Syntax

cloud-cluster link-delay *interval*

undo cloud-cluster link-delay

デフォルト

無効(0 ミリ秒)

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:遅延時間を 0 から 3000 ミリ秒の範囲で設定します。時間を 0 に設定すると、リンクダウンイベントが遅延なく通知されます。

説明

cloud-cluster link-delay はリンクダウンイベントを通知するコンテナクラスタリンクの遅延を設定します。

undo cloud-cluster link-delay はデフォルトに戻します。

I. アプリケーションのシナリオ

コンテナクラスタリンクでリンクフラッピングが発生したときにコンテナクラスタの分離と構築が頻繁に発生しないようにするには、このコマンドを使用してリンクダウンイベントの通知を遅延させるように設定します。

II. 動作メカニズム

リンクダウンイベントの通知遅延時間を設定すると、コンテナクラスタリンクがダウンした直後に、リンクダウンイベントをシステムに通知しません。遅延時間に達してもコン

テナクラスタリンクがダウンしている場合、リンクダウンイベントをシステムに通知します。

リンクアップイベントは通知遅延をさせません。コンテナクラスタリンクがアップした直後にリンクアップイベントを通知します。

III. 制限とガイドライン

このコマンドは、設定後すぐに有効になります。設定を有効にするために、**cloud-cluster configuration active** コマンドを使用する必要はありません。

例

#コンテナクラスタリンクのダウンレポートの遅延時間を 300 ミリ秒に設定します。

<Sysname> system-view

[Sysname] cloud-cluster link-delay 300

3.1.6 cloud-cluster member

Syntax

cloud-cluster member *member-id*

undo cloud-cluster member *member-id*

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id:クラスタ内のデバイスのメンバ ID を 1~2 の範囲で指定します。

説明

cloud-cluster member を使用して、cloud cluster member view に入ります。

undo cloud-cluster member を使用して、cloud cluster member view のすべての設定を削除します。

I. アプリケーションのシナリオ

メンバ ID は、クラスタ内のデバイスを識別するために使用される一意の識別子です。

II. 操作メカニズム

このコマンドは、すでに設定されているメンバ ID の cloud cluster member view に移行する場合にのみ使用できます。デバイスのメンバ ID を編集するには、**cloud-cluster member renumber** コマンドを使用します。

例

#メンバ ID 1 のデバイスの cloud cluster member view に移行します。

<Sysname> system-view

[Sysname] cloud-cluster member 1

[Sysname-ccluster-member-1]

関連コマンド

- cloud-cluster member renumber
- cloud-cluster configuration active

3.1.7 cloud-cluster member renumber

Syntax

cloud-cluster member *member-id* **renumber** *new-member-id*

undo cloud-cluster member *member-id* **renumber**

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

member-id:デバイスの現在のメンバ ID を 1~2 の範囲で指定します。

new-member-id:デバイスの新しいメンバ ID を 1~2 の範囲で指定します。

説明

cloud-cluster member renumber を使用して、デバイスのメンバ ID を編集します。

undo cloud-cluster member renumber メンバ番号を使用して、デバイスのメンバ ID の編集を削除します。

I. アプリケーションのシナリオ

メンバ ID がすでにクラスタ内にあるデバイスのメンバ ID と同じ場合、新しいデバイスをクラスタに追加することはできません。デバイスをクラスタに追加するには、このコマンドを使用してメンバ ID を異なる ID に変更します。

II. 制限とガイドライン

このコマンドは、member ID view の設定を新しい member ID view に引き継ぐことができます。設定を有効にするには、設定を保存してデバイスを再起動します。

undo cloud-cluster member renumber コマンドは、再起動前の **cloud-cluster member renumber** コマンドによって設定された新しいメンバ ID のみ削除できます。

このコマンドを実行した後、他のクラウドクラスタ設定とともに設定を有効にするには、**cloud-cluster configuration active** コマンドを実行する必要があります。

例

#デバイスメンバ ID を 1 から 2 に変更します。

<Sysname> system-view

[Sysname] cloud-cluster member 1 renumber 2

```
This command will take effect after the cloud cluster configuration is activated. The command might result in configuration change or loss when it takes effect. Continue? [Y/N]:y
```

[Sysname]

関連コマンド

- cloud-cluster configuration active
- cloud-cluster member

3.1.8 cloud-cluster service-cluster domain

Syntax

cloud-cluster service-cluster domain *domain-id*

undo cloud-cluster service-cluster domain

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-id:コンテナクラスタのドメイン ID を指定します。指定できる値の範囲は 0~4294967295 です。

説明

cloud-cluster service-cluster domain を使用して、各メンバデバイスまたはコンテナクラスタにコンテナクラスタドメイン ID を割り当てます。

undo cloud-cluster service-cluster domain を使用して、デフォルトに戻します。

I. アプリケーションのシナリオ

同じクラウドクラスタネットワークに複数のコンテナクラスタを展開できます。1 つのコンテナクラスタが 1 つのコンテナクラスタドメインを形成します。コンテナクラスタドメイン ID は、コンテナクラスタを一意に識別し、コンテナクラスタ同士の干渉を防ぎます。コンテナクラスタには、1 つのコンテナクラスタドメイン ID しかありません。ネットワーク計画に従ってコンテナクラスタのドメイン ID を変更し、ランダムな変更は避けてください。

あるコンテナクラスタが LACP MAD の中間デバイスとして別のコンテナクラスタを使用している場合、正しくクラスタの分割を検出するには、2 つのコンテナクラスタに異なるドメイン ID を割り当てる必要があります。誤って検出した場合は、コンテナクラスタが分離されます。

II. 制限とガイドライン

このコマンドを実行してコンテナクラスタドメイン ID を設定し、その他のクラウドクラスタ設定を行った後、**cloud-cluster configuration active** コマンドを実行してクラウドクラスタ設定を有効化する必要があります。

例

#コンテナクラスタドメイン ID を 1 に設定します。

<Sysname> system-view

[Sysname] cloud-cluster service-cluster domain 1

```
The configuration will take effect at the next startup.
Operation succeeded.
```

関連コマンド

- cloud-cluster configuration active
- cloud-cluster enable

3.1.9 cloud-cluster service-cluster mac-address persistent

Syntax

cloud-cluster service-cluster mac-address persistent { **always** | **timer** }

undo cloud-cluster service-cluster mac-address persistent

デフォルト

timer

View

System view

定義済みユーザロール

network-admin

パラメータ

always:コンテナクラスタのブリッジ MAC アドレスを保持できるようにします。ブリッジ MAC アドレス所有者が離脱しても、コンテナクラスタのブリッジ MAC アドレスは変更されません。

timer:ブリッジ MAC アドレスの所有者が離脱してから 6 分間、コンテナクラスタのブリッジ MAC アドレスが変更されないようにします。制限時間内にアドレス所有者が再びコンテナクラスタに参加した場合は、コンテナクラスタのブリッジ MAC アドレスは変更されません。制限時間内にアドレス所有者が参加しなかった場合、コンテナクラスタはプライマリコンテナのブリッジ MAC アドレスを新しいブリッジ MAC アドレスとして変更します。

説明

cloud-cluster service-cluster mac-address persistent を使用して、コンテナクラスタのブリッジ MAC アドレスの保持設定をします。

undo cloud-cluster service-cluster mac-address persistent を使用して、ブリッジ MAC アドレスの保持設定をデフォルトに戻します。

I. アプリケーションのシナリオ

コンテナクラスタは、そのプライマリコンテナのブリッジ MAC アドレスをコンテナクラスタのブリッジ MAC アドレスとして使用します。プライマリコンテナが変更されると、コンテナクラスタのブリッジ MAC アドレスが変更されます。一部のプロトコル(たとえばSTP)では、デバイスの識別にコンテナクラスタのブリッジMACアドレスが使用され、ブリッジ MAC アドレスの変更によって一時的なトラフィックの中断が発生することがあります。このコマンドを使用して、コンテナクラスタのブリッジ MAC アドレスを保持することができます。

II. 動作メカニズム

- ブリッジ MAC アドレスの所有者が離脱してから 6 分間、コンテナクラスタのブリッジ MAC アドレスが変更されないように設定できます。アドレス所有者が 6 分以内にコンテナクラスタに再び参加した場合、コンテナクラスタのブリッジ MAC アドレスは変更されません。アドレス所有者が 6 分以内に参加しなかった場合、コンテナクラスタはプライマリコンテナのブリッジ MAC アドレスをコンテナクラスタのブリッジ MAC アドレスとして使用します。
- コンテナクラスタのブリッジ MAC アドレスを保持する設定ができます。アドレスの所有者が離脱した後、コンテナクラスタのブリッジ MAC アドレスは変更されません。
- このコマンドを使用しない場合、ブリッジ MAC アドレスの所有者が離脱すると、すぐにコンテナクラスタはブリッジ MAC アドレスを変更します。コンテナクラスタは、現在のプライマリコンテナのブリッジ MAC アドレスをコンテナクラスタブリッジの MAC アドレスとして使用します。

III. 制限とガイドライン

2 台のメンバコンテナのブリッジ MAC アドレスが同じ場合、コンテナクラスタの構築は失敗します。コンテナクラスタブリッジ MAC アドレスは、コンテナクラスタのマージには影響しません。メンバコンテナのブリッジ MAC とコンテナクラスタブリッジ MAC は **display cloud-cluster service-cluster container verbose** コマンドで確認することができます。

コンテナクラスタに異なるメンバデバイスのインタフェースを割り当てたリンクアグリゲーショングループがある場合は、**undo cloud-cluster service-cluster mac-address persistent** コマンドを使用しないでください。このコマンドを使用すると、通信に断が発生する可能性があります。

このコマンドは、設定後すぐに有効になります。設定を有効にするために、**cloud-cluster configuration active** コマンドを使用する必要はありません。

例

#コンテナクラスタのブリッジ MAC アドレスを保持できるようにします。

<Sysname> system-view

[Sysname] cloud-cluster service-cluster mac-address persistent always

3.1.10 cloud-cluster service-cluster mad domain

Syntax

cloud-cluster service-cluster mad domain *domain-id*

undo cloud-cluster service-cluster mad domain

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-id: MAD ドメイン ID を 0~4294967295 の範囲で指定します。

説明

cloud-cluster service-cluster mad domain を使用して、コンテナクラスタに MAD ドメイン ID を割り当てます。

undo cloud-cluster service-cluster mad domain を使用して、デフォルトに戻します。

I. 動作メカニズム

コンテナクラスタの MAD ドメイン ID は、MAD にのみ使用されます。コンテナは、MAD パケットを受信すると、パケット内の MAD ドメイン ID をローカルの MAD ドメイン ID と比較します。両者が同じ場合は、パケットを処理します。クラウドクラスタ内のすべてのコンテナに同じ MAD ドメイン ID を割り当てる必要があります。クラスタの分離検出を正常に行うためには、異なるクラウドクラスタ内のコンテナには異なる MAD ドメイン ID を割り当てます。

コンテナクラスタには、1 つの MAD ドメイン ID しかありません。MAD ドメイン ID は、**cloud-cluster service-cluster mad domain** または **mad enable** のいずれかのコマンドを使用して変更できます。これらのコマンドを使用して構成された MAD ドメイン ID は、相互に上書きされます。ネットワーク設計に従ってコンテナクラスタの MAD ドメイン ID を変更し、無計画な変更を行わないようにします。

例

コンテナクラスタの MAD ドメイン ID に 1 を設定します。

<Sysname> system-view

[Sysname] cloud-cluster service-cluster mad domain 1

関連コマンド

- cloud-cluster enable
- cloud-cluster configuration active

3.1.11 cloudcluster-optimize wlan reliable-access

🕮 メモ：

cloudcluster-optimize wlan reliable-access コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

cloudcluster-optimize wlan reliable-access

undo cloudcluster-optimize wlan reliable-access

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

cloudcluster-optimize wlan reliable-access コマンドは WLAN アクセスのためのクラウドクラスタの最適化を有効にします。

undo cloudcluster-optimize wlan reliable-access コマンドはデフォルトに戻します。

この機能により、信頼性の高い AP およびクライアントアクセスを保証します。この機能は、クラウドクラスタマスタの選択、新しいメンバの参加、クラウドクラスタメンバロールの変更を加速し、クラウドクラスタイベントによって AP およびクライアントのアクセスが不安定になることを防ぎます。

例

#信頼性の高い WLAN アクセスのためのクラウドクラスタの最適化を有効にします。

<Sysname>system-view

[Sysname] cloudcluster-optimize wlan reliable-access

3.1.12 cluster-link bind interface

Syntax

cluster-link [**control** | **data**] **bind interface** *interface-type interface-number*

undo cluster-link [**control** | **data**] **bind interface** *interface-type interface-number*

デフォルト

設定なし

View

Cloud cluster member view

定義済みユーザロール

network-admin

パラメータ

control | **data** :制御リンクまたはデータリンクとして動作するコンテナクラスタリンクを指定します。このキーワードを指定しない場合、コンテナクラスタリンクは制御およびデータリンクとして動作します。

- **control**:制御リンクとして動作するリンクを指定します。制御リンクは、クラウドクラスタ内のデバイスのクラスタプロトコルパケットを転送します。
- **data**:データリンクとして動作するリンクを指定します。データリンクは、クラウドクラスタ内のデバイスのサービスパケットを転送します。

interface-type interface-number:物理インタフェースのタイプと番号を指定します。

説明

コンテナクラスタリンクに物理インタフェースを割り当てるには、**cluster-link bind interface** を使用します。

コンテナクラスタリンクから物理インタフェースの割り当てを解除するには、**undo cluster-link bind interface** を使用します。

⚠ **注意:**

undo cluster-link bind interface コマンドを実行すると、クラスタが分割されることがあります。このコマンドは慎重に使用してください。

I. アプリケーションのシナリオ

物理クラスタは、メンバ IP アドレスに基づいてレイヤ 3 で通信します。メンバ IP 間のルートが到達可能である限り、物理クラスタはプロトコルメッセージを交換し、動作を維持できます。

コンテナクラスタを使用するには、このコマンドを使用して物理インタフェースを割り当てる必要があります。コンテナクラスタリンクには、1 つの制御リンクと 1 つのデータリンクが必要です。割り当てた物理インタフェースによって制御パケットとデータパケットを転送します。制御リンクとデータリンクには同じ物理インタフェースを指定することも可能です。

II. 動作メカニズム

このコマンドを実行すると指定されたインタフェースは自動的にシャットダウンされ (**shutdown** コマンドの実行と同じ効果) 、割り当てられた物理インタフェースをクラスタ物理インタフェースに切り替えます。切り替えに成功すると自動的にインタフェースを有効にします (**undo shutdown** コマンドの実行と同じ効果) 。インタフェースの設定はデフォルト状態に変更されます。

III. 制限とガイドライン

このコマンドを設定した後、クラスタ物理インタフェースのリンクタイプを変更するには、まずコンテナクラスタリンクからインタフェースの割り当てを解除して、リンクタイプを変更する必要があります。

このコマンドを実行した後、他のクラウドクラスタ設定とともに設定を有効にするには、**cloud-cluster configuration active** コマンドを実行する必要があります。

コンテナクラスタリンクに物理インタフェースを割り当てる場合は、次のガイドラインに従ってください。

- 管理インタフェースを除く物理インタフェースを割り当てることができます。
- 最大 8 つの物理インタフェースを割り当てることができます。
- 複数の物理インタフェースを割り当てる場合は、次のいずれかの方法を使用します。
  - すべての物理インタフェースを制御リンクおよびデータリンクとして動作させます。この場合、すべての **cluster-link bind interface** コマンドにキーワード **control** あるいは **data** を指定しないでください。
  - 一部の物理インタフェースを制御リンクとして動作させ、その他の物理インタフェースをデータリンクとして動作させるように指定します。コンテナクラスタが正しく動作するように、デバイスに制御リンクとデータリンクの両方があることを確認してください。
- 複数の物理インタフェースを割り当てる場合は、同じタイプのコンテナクラスタリンクに割り当てる物理インタフェースの帯域幅が同じであることを確認してください。たとえば、制御リンクはすべて 1GE インタフェースに割り当て、データリンクはすべて 10 GE インタフェースに割り当てます。

例

#クラスタリンクにインタフェース GigabitEthernet 1/0/1 を割り当てます。

<Sysname> system-view

[Sysname] cloud-cluster member 1

[Sysname-ccluster-member-1] cluster-link bind interface gigabitethernet 1/0/1

```
The system will shut down and then bring up the interface. Continue? [Y/N]: y
```

#物理インタフェースをクラスタリンクから割り当て解除します。

<Sysname> system-view

[Sysname] cloud-cluster member 1

[Sysname-ccluster-member-1] undo cluster-link bind interface GigabitEthernet 1/0/1

```
Be cautious. If this is the only link in the cluster control channel, the
unbind operation will cause the cloud cluster to split. Continue anyway? [Y/N]:
y
```

関連コマンド

- cloud-cluster configuration active
- cloud-cluster member

3.1.13 display cloud-cluster

Syntax

display cloud-cluster [**member** *member-id*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

member *member-id*:クラスタ内のメンバ ID を指定します。*member-id* 引数の値の範囲は 1~2 です。

verbose:物理クラスタの詳細情報を表示します。物理クラスタの簡単な情報を表示する場合は、このキーワードを指定しないでください。

説明

物理クラスタに関する情報を表示するには、**display cloud-cluster** を使用します。

例

#物理クラスタに関する簡単な情報を表示します。

<Sysname> display cloud-cluster

```
Manager list:
Member ID    Role       Member IP     State      Heartbeat(ms)
1           Leader     1.1.1.1      online     0
2           Follower   1.1.1.2      online     700
```

```
Worker list:
Member ID    State      Heartbeat(ms)    Joined at
1           online     100            2023/1/2 22:10:34
2           online     200            2023/1/2 22:10:34
```

#物理クラスタの詳細情報を表示します。

<Sysname> display cloud-cluster verbose

```
Member ID        : 1
  Role           : Manager(Leader)
  Member IP      : 1.1.1.1/24
  Join-cluster IP : 1.1.1.1
  Heartbeat(ms)   : 700
  Listen port     : 3536
  Joined at       : 2023/1/2 22:10:34
  Container ID    : 1
    Container UUID: 0cfadd7138c6
    Created at    : 2023/1/2 22:10:34
    Image         : cd934004f53f
    Name          : cluster1
    Location      : 1
    State         ：Normal
Member ID        : 2
  Role           : Manager(Follower)
  Member IP      : 1.1.1.2/24
  Join-cluster IP : 1.1.1.1
  Heartbeat(ms)   : 600
  Listen port     : 3536
  Joined at       : 2023/1/2 22:10:34
  Container ID    : 2
    Container UUID: df687a7d4dfa
    Created at    : 2023/1/2 22:10:34
    Image         : cd934004f53f
    Name          : cluster2
    Location      : 2
    State         : Normal
```

表 3-1 コマンド出力

フィールド	説明
Manager list	マネージャーメンバ情報。
Worker list	ワーカーメンバ情報。

フィールド	説明
Member ID	クラスタメンバID。メンバIDで物理デバイスを識別できます。
Role	クラスタ内のデバイスの役割: ● **Manager (Leader)** :デバイスはリーダーマネージャであり、ワーカーです。 ● **Manager (Follower)** :デバイスはフォロワーマネージャであり、ワーカーです。 ● **Manager (Candidate)** :リーダーの選出が進行中です。デバイスの役割は決定されていません。
Member IP	メンバデバイスのメンバIPアドレス。
Join IP	メンバデバイスがクラスタへの参加に使用したクラスタIPアドレス。
Heartbeat(ms)	他のクラスタメンバとの最後のハートビート交換からの経過時間（ミリ秒単位）。
Listen port	クラスタ内の他のメンバデバイスからのパケットを受信するポート。このポートにより、クラスタ内のメンバデバイス間のパケット交換が保証されます。
Joined at	メンバデバイスがクラスタに参加した時刻。サポートされている時刻形式は次のとおりです。 ● YYYY-MM-DD HH:MM:SS ● YYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYY-MM-DD HH:MM:SS UTC±HH:MM ● YYY-MM-DD HH:MM:SS DST **UTC±HH:MM**は、タイムゾーンが**clock timezone**コマンドで設定されていることを示します。**DST**は、サマータイムが**clock summer-time**コマンドで設定されていることを示します。
Container ID	メンバデバイスで実行されているコンテナのID。
Container UUID	Linuxシステムがコンテナに割り当てたUUID。コンテナUUIDは内部使用専用です。

フィールド	説明
Created at	コンテナが作成された時刻。サポートされている時刻形式は次のとおりです。 • YYYY-MM-DD HH:MM:SS • YYY-MM-DD HH:MM:SS UTC±HH:MM DST • YYY-MM-DD HH:MM:SS UTC±HH:MM • YYY-MM-DD HH:MM:SS DST **UTC±HH:MM**は、タイムゾーンが**clock timezone**コマンドで設定されていることを示します。**DST**は、サマータイムが**clock summer-time**コマンドで設定されていることを示します。
Image	コンテナの起動に使用されるイメージの名前。
Name	コンテナ名。
Location	コンテナのメンバデバイス。メンバデバイスのIDが表示されます。
State	コンテナの実行状態: • **Normal**:コンテナは正常に動作しています。 • **Mad**:2つのプライマリコンテナが存在します。 • **Isolate**:一部のキーインデックスが正しくないため、コンテナが分離されています。

関連コマンド

- **cloud-cluster member**

3.1.14 display cloud-cluster configuration

Syntax

display cloud-cluster configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

クラウドクラスタ設定情報を表示するには、**display cloud-cluster configuration** を使用します。

例

#クラウドクラスタの設定情報を表示します。

<Sysname> display cloud-cluster configuration

```
Cloud-cluster: Enabled
Service cluster domain ID: 0
MAC persistent for service cluster: Always
Cloud-cluster hello timeout: 3 s
Service-cluster hello timeout: 5 s

Member ID: 1
  Role: Manager
  Member IP: 1.1.1.1/24
  Join-cluster IP: 1.1.1.1
  Bind interfaces:
    Control links: GigabitEthernet1/0/1
              GigabitEthernet1/0/2
    Data links: GigabitEthernet1/0/3
  Member ID at next startup: 1
Member ID: 2
  Role: Manager
  Member IP: 1.1.1.2/24
  Joined IP address: 1.1.1.1
  Cluster-link interfaces:
    Control links: GigabitEthernet1/0/1
    Data links: GigabitEthernet1/0/2
  Member ID at next startup: 3
```

表 3-2 コマンド出力

フィールド	説明
Cloud-cluster	物理クラスタモードの有効状態
Domain ID	コンテナクラスタのドメインID。コンテナクラスタは、ドメインIDで識別できます。

フィールド	説明
MAC persistent	ブリッジMACアドレスの保持設定。サポートされる値は次のとおりです。 • **None**:元のアドレスの所有者が離脱するとすぐに、現在のプライマリのブリッジMACアドレスによって元のブリッジMACアドレスが変更されます。 • **Always**:アドレス所有者が離脱した後も、クラスタのブリッジMACアドレスは変更されません。 • **Timer**:アドレスの所有者が離脱してから6分間、クラスタのブリッジMACアドレスは変更されません。
Member ID	クラスタメンバID。メンバIDで物理デバイスを識別できます。
Role	クラスタ内のメンバの役割。
Member IP	メンバのIPアドレス。
Join-cluster IP address	メンバがクラスタへの参加に使用したクラスタIPアドレス。
Bind interfaces	クラスタの確立に使用される物理インタフェース。
Control links	制御リンクを提供する物理インタフェース。
Data links	データリンクを提供する物理インタフェース。
Cloud-cluster hello timeout	物理クラスタのメンバのhelloタイムアウト時間（ミリ秒単位）。
Service-cluster hello timeout	コンテナクラスタのメンバのhelloタイムアウト時間（ミリ秒単位）。

3.1.15 display cloud-cluster service-cluster container

Syntax

display cloud-cluster service-cluster container [*container-id*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

container-id:コンテナを ID で指定します。*container-id* 引数の値の範囲は 1~2 です。コンテナ ID を指定しない場合、このコマンドはコンテナクラスタ内のすべてのコンテナに関する情報を表示します。

verbose:コンテナの詳細情報を表示します。簡単なコンテナ情報を表示するには、このキーワードを指定しないでください。

説明

コンテナクラスタのコンテナ情報には、**display cloud-cluster service-cluster container** を使用します。

例

#コンテナクラスタ内のすべてのコンテナに関する簡単な情報を表示します。

<Sysname> display cloud-cluster service-cluster container

```
Container ID    Slot ID     Member ID    Role      Status
1               1           1            Master    Online
2               2           2            Standby   Online
```

#コンテナクラスタ内のすべてのコンテナに関する詳細情報を表示します。

<Sysname> display cloud-cluster service-cluster container verbose

```
Service-cluster name: System
  Domain ID        : 0
  Cluster Bridge MAC: 00e0-fc00-1001
  Container ID   : 1
    Member ID    : 1
    Slot ID      : 1
    Health       : Healthy(100)
    Bridge MAC   : 00e0-fc00-1001
    CPU MAC      : 00f0-fc00-1001
    Control links: GigabitEthernet1/0/1(UP)
                   GigabitEthernet1/0/2(DOWN)
    Data links   : GigabitEthernet1/0/3(UP)
    Cluster connection : Reachable
    Status       : Online
    Self hello timeout (ms)  : N/A
    Master hello timeout (ms): N/A
```

表 3-3 コマンド出力

フィールド	説明
Service-cluster	コンテナクラスタの名前。**System**のみがサポートされています。
Domain ID	コンテナクラスタのドメインID。コンテナクラスタは、ドメインIDで識別できます。
Cluster Bridge MAC	クラスタのクラスタブリッジMACアドレス。
Container ID	コンテナID。クラスタは、コンテナの作成時にコンテナにIDを割り当てます。
Member ID	クラスタメンバID。メンバIDで物理デバイスを識別できます。
Slot ID	メンバコンテナのスロットID。
Role	クラスタ内のメンバコンテナの役割: ● **Master**:プライマリコンテナ。 ● **Standby**:スタンバイコンテナ。 ● **IO**:インタフェースモジュール。
Health	システムヘルス状態: ● **Healthy (100)** :システムは正常です。 ● **Unhealthy (n)** :システムが異常です。nの値が大きくなると、システムヘルス状態が悪化しています。
Bridge MAC	メンバコンテナのブリッジMACアドレス。
CPU MAC	メンバコンテナのCPU MACアドレス。
Control links	コントロールリンクを提供する物理インタフェースとその物理状態。
Data links	データリンクを提供する物理インタフェースとその物理状態。
Cluster connection	クラウドプラットフォームのエージェントとマネージャの相互接続状態: ● **Reachable**:互いに到達可能 ● **Unreachable**:互いに到達不可能
Status	コンテナの実行状態: ● **Online**:コンテナはオンラインです。 ● **Offline**:コンテナはオフラインです。 ● **MAD down**:コンテナは禁止されています。

フィールド	説明
Self hello timeout (ms)	コンテナのhelloタイムアウト時間（ミリ秒単位）。コンテナは、特定の間隔でプライマリコンテナにhelloパケットを送信します。プライマリコンテナのこのフィールドには、**N/A**が表示されます。
Master hello timeout (ms)	プライマリコンテナのhelloタイムアウト時間（ミリ秒単位）。プライマリコンテナは、特定の間隔でhelloパケットをコンテナに送信します。プライマリコンテナのこのフィールドには、**N/A**が表示されます。

関連コマンド

- cloud-cluster member

3.1.16 display mad

Syntax

display mad [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: 詳細な MAD 設定情報を表示します。このキーワードを指定しない場合、コマンドは簡単な MAD 設定情報を表示します。

説明

display mad を使用して MAD の設定を表示します。

例

#簡単な MAD 設定情報を表示します。

<Sysname> display mad

```
MAD LACP enabled.
```

#MAD 設定の詳細情報を表示します。

<Sysname> display mad verbose

```
Multi-active recovery state: No
Excluded ports (user-configured):
  Bridge-Aggregation4
  Vlan-interface999
Excluded ports (system-configured):
 physical interfaces:
    Ten-GigabitEthernet1/0/1
    Ten-GigabitEthernet1/0/2
    Ten-GigabitEthernet2/0/1
    Ten-GigabitEthernet2/0/2
  Member interfaces of excluded interface Bridge-Aggregation 4:
    Ten-GigabitEthernet1/0/4
    Ten-GigabitEthernet2/0/4
MAD LACP enabled interface: Bridge-Aggregation 1
  MAD status               : Normal
  Member ID      Port                        MAD status
  1              Ten-GigabitEthernet1/0/5      Normal
  2              Ten-GigabitEthernet2/0/5      Normal
```

表 3-4 コマンド出力

フィールド	説明
MAD LACP enabled.	LACP MADの状態。LACP MADが無効の場合、**MAD LACP disabled**と表示されます。
Multi-active recovery state	コンテナクラスタのRecovery状態: ● **Yes**:コンテナクラスタはRecovery状態です。MADは、コンテナクラスタが分離されたことを検出すると、1つのメンバコンテナによるトラフィックの転送のみ許可します。他のすべてのメンバコンテナは、Recovery状態に設定されます。Recovery状態では、MADはシステムおよびユーザが除外したインタフェースを除くクラスタ内のすべてのインタフェースをシャットダウンします。 ● **No**:コンテナクラスタはRecovery状態ではありません。すべてのメンバコンテナはアクティブであり、トラフィックを転送できます。
Excluded ports (user-configured)	メンバコンテナがRecovery状態に移行したときにシャットダウンしないように手動で設定されたインタフェース。

フィールド	説明
Excluded ports (system-configured)	コンテナクラスタがRecovery状態に移行するときにシステムによってシャットダウンされないように設定されたインタフェース。これらのインタフェースは手動で設定されません。 ● **physical interfaces**:コンテナクラスタリンクの物理インタフェース。 ● **Member interfaces of excluded interface Bridge-Aggregation** *interface-number*:リンクアグリゲーションインタフェースがMADシャットダウンアクションから除外指定されている場合は、そのリンクアグリゲーショングループのメンバインタフェース。
MAD LACP enabled interface	LACP MADが有効なインタフェース。このフィールドは、LACP MADが有効なインタフェースごとに表示されます。LACP MADが無効な場合、このフィールドには**MAD LACP disabled**が表示されます。
MAD status	LACP MAD動作ステータス: ● **Normal**:LACP MADは正常に動作しています。 ● **Faulty**:LACP MADは正常に動作していません。次の項目を確認してください。 ・LACP MADリンクのインタフェースがリンクアップしていることを確認します。 ・中間デバイスでLACPが有効で、LACP MADフレームに対応していることを確認します。 ・すべてのメンバデバイスに、LACP MADに使用されるメンバインタフェースがあることを確認します。
Member ID Port MAD status	LACP MADの詳細: ● **Member ID**:コンテナクラスタ内のメンバID。 ● **Port**:LACP MADに使用されるリンクアグリゲーショングループのメンバインタフェース。 ● **MAD status**:メンバインタフェースのLACP MAD動作状態。値には、**Normal**と**Faulty**が含まれます。

3.1.17 join-cluster

Syntax

join-cluster ip *ipv4-address*

undo join-cluster

デフォルト

設定なし

View

Cloud cluster member view

定義済みユーザロール

network-admin

パラメータ

ip *ipv 4-address*:クラスタ内のメンバデバイスの IP アドレスを指定します。

説明

join-cluster を使用してクラスタ IP アドレスを設定します。

undo join-cluster を使用して、クラスタ IP 設定を削除します。デバイスはクラスタを離れます。

I. アプリケーションのシナリオ

物理クラスタを作成するには、物理クラスタのすべてのメンバデバイスでこのコマンドの設定が必要です。デバイスを物理クラスタのリーダーとして設定するには、このコマンドを設定しないか、デバイスのメンバ IP アドレスをクラスタ IP アドレスとして使用します。このコマンドを設定せずクラウドクラスタ設定を有効にすると、デバイスは自身がリーダーとして機能するクラスタを作成します。このコマンドは、他のフォロワーデバイスで設定する必要があります。

II. 動作メカニズム

クラスタを作成する場合は、最初にリーダーとして機能するデバイスを選択し、内部クラスタ通信用のメンバ IP アドレスを選択します。次にリーダーデバイスを設定して有効にします。クラスタに他のデバイスを追加する場合は、次の注意事項に従ってください。

- ベストプラクティスとして、このコマンドでリーダーのメンバ IP アドレスを指定します。新しいデバイスは、リーダーと直接接続を確立してクラスタに参加できます。
- このコマンドでクラスタ内の別のメンバデバイスの IP アドレスを指定すると、新しいデバイスはメンバデバイスに接続要求を送信します。その後、新しいデバイスはリーダーとの接続を確立してクラスタに参加できます。

指定された IP アドレスに到達できない場合、デバイスはクラスタに参加できません。この場合、**display cloud-cluster** コマンドはクラスタ情報を表示せず、デバイス上のコンテナがマスタとしてシングルデバイスとして動作します。

デバイスを確実にクラスタから削除するには、まず **undo join-cluster** コマンドを実行してから、**cloud-cluster configuration active** コマンドを実行する必要があります。削除中に、現在のクラスタの設定、データ、およびトポロジがデバイスから削除され、コンテ

ナ関連の設定が保持されます。デバイスは、自身がリーダーとして機能するクラスタを作成し、デバイス上のコンテナがマスタとして動作します。

クラスタから分離されたメンバデバイスを追加するには、**join-cluster** コマンドを実行します。設定を保存してデバイスを再起動すると、デバイスは再びクラスタに追加されます。

このコマンドを使用して設定を保存した後、スタンドアロンモードに切り替えると、設定は無効になります。再度クラスタモードに切り替えても、設定は有効になりません。

III. 制限とガイドライン

このコマンドを実行した後、設定を他のクラウドクラスタ設定とともに有効にするには、**cloud-cluster configuration active** コマンドを実行する必要があります。

例

#クラスタ IP アドレスが 1.1.1.1 のリーダーデバイスを含むクラウドクラスタにデバイスを追加します。

<Sysname> system-view

[Sysname] cloud-cluster member 1

[Sysname-ccluster-member-1] join-cluster ip 1.1.1.1

#メンバ ID 2 のデバイスをクラスタから分離します。

<Sysname> system-view

[Sysname] cloud-cluster member 2

[Sysname-ccluster-member-2] undo join-cluster

```
Member 2 will be isolated from the cluster with its network interfaces disabled.
Continue? [Y/N]: y
```

関連コマンド

- cloud-cluster member
- cloud-cluster configuration active
- member-ip

3.1.18 mad enable

Syntax

mad enable

undo mad enable

デフォルト

無効

View

Aggregate interface view

定義済みユーザロール

network-admin

説明

LACP MAD を有効にするには、**mad enable** を使用します。

LACP MAD を無効にするには、**undo mad enable** を使用します。

LACP MAD には、MAD が中間デバイスとして機能するための拡張 LACPDU をサポートするデバイスが必要です。コンテナクラスタと中間デバイス間のすべてのクラウドクラスタメンバデバイスにまたがる LACP グループを設定する必要があります。LACP を有効にするには、リンクアグリゲーションインタフェースで **link-aggregation mode dynamic** コマンドを設定します。

あるコンテナクラスタが別のコンテナクラスタを LACP MAD の中間デバイスとして使用している場合、MAD によって分離を正しく検出するには 2 つのコンテナクラスタに異なるドメイン ID を割り当てる必要があります。誤って検出すると、コンテナクラスタが分離されます。

コンテナクラスタのドメイン ID は 1 つです。**cloud-cluster service-cluster mad domain** または **mad enable** のいずれかのコマンドを使用して、ドメイン ID を変更できます。

例

#LACP を有効にした Bridge-Aggregation 1 で LACP MAD を有効にします。

<Sysname> system-view

[Sysname] interface bridge-aggregation 1

[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic

[Sysname-Bridge-Aggregation1] mad enable

```
You need to assign a domain ID (range: 0-4294967295)
[Current domain ID is: 0]: 1
The assigned domain ID is: 1
```

関連コマンド

- cloud-cluster service-cluster domain

3.1.19 mad exclude interface

Syntax

mad exclude interface *interface-type interface-number*

undo mad exclude interface *interface-type interface-number*

デフォルト

システムによって自動的に除外されたインタフェースを除き、すべてのインタフェースは、メンバコンテナが Recovery 状態に移行するとシャットダウンされます。システムは、次のネットワークインタフェースを自動的にシャットダウンから除外します。

- コンテナクラスタリンクの物理インタフェース。
- ユーザによって除外設定されたリンクアグリゲーションインタフェースのメンバインタフェース

View

System view

定義済みユーザロール

network-admin

パラメータ

*interface-type interface-number:*タイプと番号でインタフェースを指定します。

説明

コンテナクラスタが Recovery 状態に移行するときに、インタフェースがシャットダウンされないようにするには、**mad exclude interface** を使用します。

Recovery 状態に移行するときに、コンテナクラスタがインタフェースをシャットダウンするように設定するには、**undo mad exclude interface** を使用します。

リモートアクセスによる管理目的のためにインタフェースをアップ状態に保つ必要がある場合など特別な用途で接続が必要なインタフェースがある場合は、そのインタフェースをシャットダウンアクションから除外します。誤ったトラフィック転送を避けるためのベストプラクティスとして、特別な用途に使用されるインタフェースのみ除外設定をしてください。

MAD によってシャットダウンされたインタフェースは、コンテナクラスタリンクが復旧して、再びクラスタに参加するためにメンバデバイスが再起動するときにリンクアップします。クラウドクラスタリンクが回復する前にアクティブなメンバコンテナで障害が発生した場合は、非アクティブなメンバコンテナで **mad restore** コマンドを使用して、非アクティブなメンバコンテナのインタフェースを回復させます。このコマンドは、MAD によってシャットダウンされたすべてのインタフェースをリンクアップさせます。

例

#MAD ステータスが Recovery に移行するときに、GigabitEthernet 1/0/1 がシャットダウンされないようにします。

<Sysname> system-view

[Sysname] mad exclude interface gigabitethernet 1/0/1

関連コマンド

- mad restore

3.1.20 mad restore

Syntax

mad restore

View

System view

定義済みユーザロール

network-admin

説明

mad restore を使用して、Recovery 状態のコンテナクラスタのシャットダウンポートを復旧します。

コンテナクラスタの分離が復旧する前にアクティブなコンテナクラスタが機能しない場合は、このコマンドを使用して Recovery 状態のコンテナクラスタを復旧させます。復旧されたコンテナクラスタがアクティブなコンテナクラスタの役割を引き継ぎます。

例

#Recovery 状態のコンテナクラスタを復旧させます。

<Sysname> system-view

[Sysname] mad restore

```
This command will restore the device from multi-active conflict state.
Continue? [Y/N]:Y
Restoring from multi-active conflict state, please wait...
```

3.1.21 member-ip

Syntax

member-ip *ipv4-addr mask-length*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv4-addr:メンバデバイスのメンバ IP アドレスを指定します。アドレスはループアドレス、ブロードキャストアドレス、マルチキャストアドレス、または 0.X.X.X にすることはできません。

mask-length:メンバ IP アドレスのマスク長を 1 から 31 の範囲で指定します。

説明

デバイスのメンバ IP アドレスを指定するには、**member-ip** を使用します。

I. アプリケーションシナリオ

メンバ IP アドレスは、物理クラスタ内のメンバデバイス間で物理クラスタプロトコルパケット通信をするために使用されます。物理クラスタ内のすべてのメンバデバイスは、メンバ IP アドレスを設定する必要があります。

II. 制限とガイドライン

メンバ IP が通常のデータ通信を行うサブネットとは異なることを確認します。

クラスタ内に追加するすべてデバイスのメンバ IP アドレスが同じサブネット内にあることを確認します。

物理クラスタ構築後はメンバ IP アドレスは削除できず、他のメンバデバイスのメンバ IP アドレスと同じサブネット内のアドレスへの変更のみできます。メンバ IP アドレスを異なるサブネット内のアドレスに変更するには、まず、**undo join-cluster** および **cloud-cluster configuration active** コマンドを順番に実行して、デバイスを物理クラスタから削除します。

このコマンドを実行した後、他のクラウドクラスタ設定とともに設定を有効にするには、**cloud-cluster configuration active** コマンドを実行する必要があります。

例

#メンバ ID 1 のデバイスのメンバ IP アドレスを 1.1.1.1/24 に設定します。

<Sysname> system-view

[Sysname] cloud-cluster member 1

[Sysname-ccluster-member-1] member-ip 1.1.1.1 24

関連コマンド

- cloud-cluster configuration active
- cloud-cluster member
- join-cluster

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

15. セキュリティ

本マニュアルは以下に示す章で構成されています。

01- ACL

02- Packet filter

03-タイムレンジ

04-パスワード管理

05-公開鍵

06-SSH

07-SSL

08-接続制限

09-TCP フラグメントアタックプロテクション

10-IP ソースガード

11-ARP アタックプロテクション

目次

このセクションのページは **15-x-x** です。

1 章 ACL 1-1
1.1 ACL 設定コマンド 1-1
1.1.1 acl 1-1
1.1.2 acl copy 1-3
1.1.3 description 1-4
1.1.4 display acl 1-5
1.1.5 reset acl counter 1-6
1.1.6 rule (IPv4 advanced ACL view) 1-7
1.1.7 rule (IPv4 basic ACL view) 1-15
1.1.8 rule (Layer 2 ACL view) 1-17
1.1.9 rule comment 1-20
1.1.10 step 1-21

1章 ACL

1.1 ACL設定コマンド

1.1.1 acl

Syntax

コマンド形式 1

acl number *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

undo acl number *acl-number*

コマンド形式 2

acl { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

undo acl { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

デフォルト

ACL は存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

basic:基本 ACL を作成するように指定します。

advanced:拡張 ACL を作成するように指定します。

mac:レイヤ 2 ACL の作成を指定します。

number acl-number:ACL の番号を指定します。

acl-number は ACL の番号を表し、次の ACL タイプを表す値の範囲を取ります。

- 2000~2999:基本 ACL を示す。
- 3000~3999:拡張 ACL を表します。
- 4000~4999:レイヤ 2 ACL を表します。

name acl-name:ACL の名前を指定します。acl-name は、ACL の名前を表す 1~63 文字の文字列です。大文字と小文字は区別されず、a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

match-order {auto |config }:規則の照合順序を指定します。auto は規則の照合が自動ソート(つまり「深さ優先」という原則です)の順序で行われることを示し、config は設定された順序で行われることを示します。デフォルトでは、規則の照合順序は構成順序です。ユーザー定義 ACL ではこのパラメータはサポートされておらず、ルールの一致順序は設定された順序のみです。

all:指定したタイプのすべての ACL。

説明

acl コマンドを使用して ACL を作成し、ACL view に入力します。指定した ACL がすでに存在する場合は、ACL view に直接進みます。

undo acl コマンドは、指定された ACL またはすべての ACL を削除します。

番号で作成された ACL は、次のコマンドでビューに表示できます。

- acl number acl-number;
- acl { {advanced | basic } | mac } acl-number。

ACL 内にルールが存在しない場合は、このコマンドを使用して ACL のルール一致順序を変更できます。それ以外の場合は変更できません。

ACL ルールの一致に、IP 5 タプル(送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号、トランスポート層プロトコル)、ICMP メッセージ、または ICMPv6 メッセージのメッセージタイプとメッセージコード情報、VPN インスタンス、ログアクション、および期間以外の一致が含まれている場合、デバイスは ACL が一致するメッセージを転送するときにスロー転送プロセスを有効にします。低速転送では、デバイスは制御プレーンにメッセージを送信し、メッセージに対応するエントリ情報を計算します。低速転送プロセスを実行すると、デバイスの転送能力が低下します。

例

#IPv4 ベース ACL を作成し、そのビューに 2000 を入力します。

<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000]

#IPv4 基本 ACL を作成し、その名前を flow と指定してビューに移動します。

<Sysname> system-view
[Sysname] acl basic name flow
[Sysname-acl-ipv4-basic-flow]

#IPv4 拡張 ACL を 3000 という番号で作成し、表示します。

<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000]

#4000 という番号のレイヤ 2 ACL を作成し、ビューに移動します。

<Sysname> system-view
[Sysname] acl mac 4000

[Sysname-acl-mac-4000]

#flow という名前のレイヤ 2 ACL を作成し、そのビューに入ります。

<Sysname> system-view
[Sysname] acl mac name flow
[Sysname-acl-mac-flow]

関連コマンド

- **display acl**

1.1.2 acl copy

Syntax

acl [**mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

View

System view

定義済みユーザロール

network-admin

パラメータ

mac:ACL タイプをレイヤ 2 ACL に指定します。

source-acl-number:存在する必要があるソース ACL の番号を指定します。このパラメータの範囲と、それが表す ACL のタイプは次のとおりです。

- 2000~2999:基本 ACL を示す。
- 3000~3999:拡張 ACL を表します。
- 4000~4999:レイヤ 2 ACL を表します。

name source-acl-name:存在する必要があるソース ACL の名前を指定します。source-acl-name は 1~63 文字の文字列で、大文字と小文字は区別されません。

dest-acl-number:存在しない必要がある宛先 ACL の番号を指定します。このパラメータの範囲と、それが表す ACL のタイプは次のとおりです。

- 2000~2999:基本 ACL を示す。
- 3000~3999:拡張 ACL を表します。
- 4000~4999:レイヤ 2 ACL を表します。

name dest-acl-name:存在しない必要がある宛先 ACL の名前を指定します。dest-acl-name は 1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

説明

acl copy コマンドを使用して、新しい ACL をコピーして生成します。

宛先 ACL のタイプは、ソース ACL のタイプと同じである必要があります。

ACL の番号または名前が異なることを除いて、新しく生成された ACL (インテント ACL) の照合順序、ルール照合ソフトウェアの統計機能のオン、ルール番号のステップサイズ、含まれるルール、ルールの説明情報、および ACL の説明情報は、ソース ACL と同じです。

例

#既存の IPv4 ベース ACL 2001 をコピーして、同じタイプの新しい番号 2002 の ACL を生成します。

<Sysname> system-view
[Sysname] acl copy 2001 to 2002

#既存の IPv4 ベース ACL test をコピーして、paste という同じタイプの ACL を生成します。

<Sysname> system-view
[Sysname] acl copy name test to name paste

1.1.3 description

Syntax

description *text*

undo description

デフォルト

ACL には記述情報がありません。

View

IPv4 basic/advanced ACL view

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

text:ACL の説明を示す 1~127 文字の文字列で、大文字と小文字が区別されます。

説明

description コマンドを使用して、ACL の説明情報を設定します。

undo description コマンドを使用して、ACL の説明情報を削除します。

例

#IPv4 のための基本的な ACL 2000 設定説明情報。

<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.

関連コマンド

- **display acl**

1.1.4 display acl

Syntax

display acl [**mac**] { *acl-number* | **all** | **name** *acl-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac:ACL タイプをレイヤ 2 ACL に指定します。

acl-number:指定した数の ACL の設定と動作を表示します。acl-number は ACL の番号を表し、次の ACL タイプを表す値の範囲を取ります。

- 2000~2999:基本 ACL を示す。
- 3000~3999:拡張 ACL を表します。
- 4000~4999:レイヤ 2 ACL を表します。

all:指定したタイプのすべての ACL の設定と動作を表示します。

name acl-name:指定した名前の ACL の設定と動作を表示します。acl-name は ACL の名前で、大文字と小文字を区別しない 1~63 文字の文字列です。

説明

display acl コマンドを使用して、ACL の設定と動作を表示します。

このコマンドは、ACL 内のルールを実際の照合順に並べます。つまり、ACL のルール照合順が設定順の場合、各ルールは番号順に並べられます。ACL のルール一致順序が自動順序である場合、各ルールは「深さ優先」の原則に従って深い順に並べられます。

例

#IPv4 基本 ACL 2001 の構成と動作を表示します。

<Sysname> display acl 2001

Basic IPv4 ACL 2001 named test, 2 rules, match-order is auto,

This is an IPv4 basic ACL.

ACL's step is 5、start ID is 0

rule 5 permit source 1.1.1.1 0

rule 5 comment This rule is used on GigabitEthernet1/0/1.

rule 10 deny source 10.0.0.101 0 counting time-range a3 (Active)

#IPv4 Advanced ACL 3001 の構成と動作を表示します。

<Sysname> display acl 3001

Advanced IPv4 ACL 3001、2 rules

ACL's step is 5、start ID is 0

rule 0 permit tcp

rule 5 permit ip source 10.0.0.100 0 (2854 times matched)

表 1-1 display acl コマンドの表示情報の説明

フィールド	説明
Basic IPv4 ACL 2001 named test	ACLのタイプ、番号、名前
2 rules	ACLに含まれるルールの数
match-order is auto	このACLのルール照合順序は自動ソート(照合順序が構成順序の場合、このフィールドは表示されません。)です。
This is an IPv4 basic ACL.	ACLの説明
ACL's step is 5	このACLのルール番号のステップ値は5です。
start ID is 0	このACLのルール番号の開始値は0です。
rule 5 permit source 1.1.1.1 0	ルール5の具体的な内容、ソースアドレスは具体的なアドレスである.
rule 5 comment This rule is used on GigabitEthernet1/0/1.	ルール5の記述情報
Active	期間を参照する規則が有効になっています
Inactive	期間を参照するルールは有効ではありません
2854 times matched	このルールの一致回数

1.1.5 reset acl counter

Syntax

reset acl [**mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

mac:ACL タイプをレイヤ 2 ACL に指定します。

acl-number:指定した番号の ACL の統計情報をクリアします。acl-number は ACL の番号を表し、次の ACL タイプを表す値の範囲を取ります。

- 2000~2999:基本 ACL を示す。
- 3000~3999:拡張 ACL を表します。
- 4000~4999:レイヤ 2 ACL を表します。

all:指定したタイプのすべての ACL の統計情報をクリアします。

name acl-name:指定された名前 ACL の統計情報をクリアします。acl-name は ACL の名前で、大文字と小文字を区別しない 1~63 文字の文字列です。

説明

reset acl counter コマンドは、ACL の統計情報をクリアするために使用されます。

例

#IPv4 基本 ACL 2001 の統計情報をクリアします。

<Sysname> reset acl counter 2001

関連コマンド

- **display acl**

1.1.6 rule (IPv4 advanced ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | { { **precedence** | **tos** } * | **dscp** } | **fragment** | **icmp-type** | **source** | **source-port** | **time-range**] *

undo rule { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { { **precedence** | **tos** } * | **dscp** *dscp* } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] |

icmp-message } | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

デフォルト

IPv4 拡張 ACL にはルールがありません。

View

IPv4 拡張 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id:IPv4 拡張 ACL ルールの番号を 0~65534 の範囲で指定します。このパラメータが指定されていない場合、既存の最大数を超えるステップの最小倍数が、ルール番号の開始値から自動的に割り当てられます。たとえば、既存ルールの最大番号が 28,ステップサイズが 5 であれば、自動的に割り当てられる新しい番号は 30 となる。

deny:条件を満たすメッセージを拒否することを示す。

permit:条件を満たすメッセージを許可することを示す。

*protoco*l:IPv4 がホストするプロトコルのタイプを示します。次の形式で入力できます。

- 数値:0~255 の範囲;
- 名前(括弧内は対応する数字):gre (47)、icmp (1) 、igmp (2) 、ip、ipinip (4) 、ospf (89)、tcp (6) 、または udp (17)を選択できます。ip はすべてのプロトコルタイプを表します。

protocol の後に、表 1-2 に示すようなルール情報パラメータを設定することができる。

表 1-2 ルール情報パラメータ

パラメータ	カテゴリ	作用	説明
source {source-address source-wildcard |any}	送信元アドレス情報	ACLルールの送信元アドレス情報の指定	source-address:送信元IPアドレス source-wildcard:送信元IPアドレスのワイルドカードマスク(ホストアドレスは0です。) any:任意の送信元IPアドレス

パラメータ	カテゴリ	作用	説明
destination {dest-address dest-wildcard |any}	宛先アドレス情報	ACLルールの宛先アドレス情報の指定	dest-address:宛先IPアドレス dest-wildcard:宛先IPアドレスのワイルドカードマスク(ホストアドレスは0です。) any:任意の宛先IPアドレス
counting	統計	ルール・マッチング・ソフトウェア統計機能を有効にします。デフォルトはオフです。	このパラメータは、このルールの照合統計を有効にするために使用されます。
precedence precedence	メッセージ優先度	IP優先順位の指定	precedence数値の場合、範囲は0~7です。文字で表した場合、それぞれroutine, priority, immediate, flash, flash-override, critical, internet, networkに対応する.
tos tos	メッセージ優先度	ToS優先度の指定	tosは数値の場合0~15の範囲で指定します。文字で表す場合は、max-reliability (2) 、max-throughput (4) 、min-delay (8) 、min-monetary-cost (1) 、normal (0) を選択できます。

パラメータ	カテゴリ	作用	説明
dscp dscp	メッセージ優先度	DSCP優先順位の指定	dscpが数値の場合、0~63の値を取ります。記号で表す場合、af 11 (10)、af 12 (12)、af 13 (14)、af 21 (18)、af 22 (20)、af 23 (22)、af 31 (26)、af 32 (28)、af 33 (30)、af 41 (34)、af 42 (36)、af 43 (38)、cs 1 (8) 、cs 2 (16)、cs 3 (24)、cs 4 (32)、cs 5 (40)、cs 6 (48)、cs 7 (56)、default (0) 、ef (46)を選択できます。
fragment	スライス情報	シャードされていないメッセージの最初のシャードでのみ有効で、シャードされていないメッセージとシャードされているメッセージの最初のシャードでは無効です	シャーディング関連のパラメータが指定されていない場合、ルールはすべてのメッセージ(シャードされていないメッセージとシャードされたメッセージを含む各シャード)に対して有効です。

パラメータ	カテゴリ	作用	説明
time-range time-range-name	期間	この規則が有効になる期間を指定します	time-range-name:期間の名前。1~32文字の文字列で、大文字と小文字は区別されません。a~zまたはA~Zで始まる必要があります。期間が設定されていない場合、ルールは正常に作成されますが、プロンプトが表示され、期間の設定が完了するまでルールは有効になりません。期間の詳細と構成手順については、QX-W2300ACシリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*2 章 タイムレンジ*”を参照してください。

protocol が tcp (6) または udp (17)の場合は、表 1-3 に示すルール情報パラメータも設定できます。

表 1-3 TCP/UDP 固有のルール情報パラメータ

パラメータ	カテゴリ	作用	説明
source-port operator port1 [port2]	ソースポート	TCP/UDPメッセージの送信元ポート情報の定義	operatorは演算子で、lt (より小さい)、gt (より大きい)、eq (等しい)、neq (等しくない)、range (範囲内、境

パラメータ	カテゴリ	作用	説明
destination-port operator port1 [port2]	宛先ポート	TCP/UDPメッセージの宛先ポート情報の定義	界値を含む)のいずれかの値を取ります。オペランドに2つのポート番号が必要なのはオペレータrangeだけで、それ以外はオペランドに1つのポート番号が必要です port1、port2:TCPまたはUDPのポート番号。数値の場合は0~65535の範囲で指定します。TCPポート番号は、文字表記の場合、chargen (19)、bgp (179)、cmd (514)、daytime (13)、discard (9) 、dns (53)、domain (53)、echo (7) 、exec (5 12)、finger (79)、ftp (21)、ftp-data (20)、port1 (70)、port2 (101)、irc (194)、klogin (543)、kshell (544)、login (513)、lpd (515)、nntp (119)、pop 2 (109)、pop 3 (110)、smtp (25)、sunrpc (111)、tacacs (49)、talk (517)、telnet (23)、time (37)、uucp (540)、whois (43)、www (80);UDPポート番号はbiff (20)、ftp-data (19)、port1 (179)、port2 (9) 、dns (514)、chargen (13)、daytime (7) 、discard (53)、domain (53)、echo (5 12)、exec (79)、finger (21)、bootpc (110)、ntp (70)、rip (101)、snmp (194)、gopher (543)、hostname (544)、klogin (513)、kshell (515)、talk (119)、tftp (109)、time (5 12)、who (25)、login (111)
{ack ack-value |fin fin-value |psh psh-value |rst rst-value |syn syn-value |urg urg-value }*	TCPメッセージID	異なるフラグビット(ACK、FIN、PSH、RST、SYN、URGの6種類)を持つTCPメッセージに対する処理ルールを定義する.	TCPプロトコル固有のパラメータ。異なるフラグビットを持つTCPメッセージにマッチすることを表し、各valueは0または1の値をとる(0はこのフラグビットを保持しないことを意味し、1はこのフラグビットを保持することを意味します。). 1つの規則内の各マーカーの構成の組み合わせに対して、またはの規則に従って一致させます。たとえば、 ack 0 psh 1のように配置した場合、 ACKまたはPSHフラグを持たないTCPメッセージにマッチする.

パラメータ	カテゴリ	作用	説明
established	TCP接続確立ID	TCP接続メッセージに対する処理規則の定義	TCPプロトコル固有のパラメータ ACKまたはRSTフラグビットを持つTCP接続メッセージに一致することを示す

protocol が icmp (1) の場合は、表 1-4 に示すルール情報パラメータを設定することもできます。

表 1-4 ICMP 固有のルール情報パラメータ

パラメータ	カテゴリ	作用	説明
icmp-type {icmp-type icmp-code |icmp-message }	ICMPメッセージのメッセージタイプとメッセージコード情報	この規則でICMPメッセージのメッセージタイプとメッセージコード情報を指定します。	icmp-type:0~255の範囲のICMPメッセージタイプ icmp-code:0~255の範囲のICMPメッセージコード icmp-message:ICMPメッセージ名。入力可能なICMPメッセージ名と、そのメッセージタイプおよびメッセージコードとの対応は表 1-5に示す.

表 1-5 ICMP メッセージ名とメッセージタイプおよびメッセージコードの対応

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

説明

rule コマンドを使用して、IPv4 拡張 ACL のルールを作成します。

IPv4 拡張 ACL のルールまたはルールの一部を削除するには、**undo rul**e コマンドを使用します。

rule コマンドを使用して、番号を指定するルールが存在しない場合は、新しいルールを作成します。番号付けされた規則がすでに存在する場合は、古い規則が変更され、元の内容に新しい内容が追加されます。

新しく作成または変更されたルールは、既存のルールと同じ内容にすることはできません。同じ内容にすると、エラーが表示され、操作が失敗します。

ACL のルール一致順序が設定されている場合、ACL 内の既存のルールを変更できます。ACL のルール一致順序が自動ソートの場合、ACL 内の既存のルールを変更することはできません。変更しないと、エラーが表示されます。

display acl all コマンドは、既存のすべての IPv4 拡張 ACL ルールと IPv4 基本 ACL ルールを表示します。

ルールを削除する場合は、次の点に注意してください。

- **undo rule rule-id** コマンドを使用するときにオプションのパラメータを指定しないと、ルール全体が削除されます。オプションのパラメータが指定されている場合は、そのパラメータの内容のみが削除されます。
- **undo rule {deny |permit }**コマンドではルールの一部を削除できません。**undo rule {deny |permit }**コマンドを使用する場合は、既存のルールの完全な形式を入力する必要があります。

例

#IPv4 Advanced ACL 3000 のルールを次のように作成します。129.9.0.0/16 ネットワークセグメント内のホストが、202.38.160.0/24 ネットワークセグメント内のホストの WWW ポート(ポート番号は 80 です)に接続できるようにします。

<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80

#IPv4 Advanced ACL 3001 のルールを次のように作成します。IP メッセージの通過は許可しますが、192.168.1.0/24 ネットワークセグメント宛ての ICMP メッセージの通過は拒否します。

<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] rule permit ip

#IPv4 Advanced ACL 3002 のルールを次のように作成します。FTP 接続の確立と FTP データの転送は、送信側と受信側の両方で許可されます。

<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data

#IPv4 Advanced ACL 3003 用のルールを次のように作成します。SNMP メッセージと SNMP Trap メッセージは、送信側と受信側の両方で許可されます。

<Sysname> system-view
[Sysname] acl advanced 3003
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range (ACL および QoS コマンドリファレンス/期間)**

1.1.7 rule (IPv4 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **source** | **time-range**] *

undo rule { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

デフォルト

IPv4 ベース ACL にはルールがありません。

VIew

IPv4 基本 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id:IPv4 ベース ACL ルールの番号を 0~65534 の範囲で指定します。このパラメータが指定されていない場合、既存の最大数を超えるステップの最小倍数が、ルール番号の開始値から自動的に割り当てられます。たとえば、既存ルールの最大番号が 28,ステップサイズが 5 であれば、自動的に割り当てられる新しい番号は 30 となる。

deny:条件を満たすメッセージを拒否することを示す。

permit:条件を満たすメッセージを許可することを示す。

counting:ルール・マッチング・ソフトウェア統計がオンで、デフォルトでオフになっていることを示します。

fragment:フラグメント化されていないメッセージにのみ有効であり、フラグメント化されていないメッセージとフラグメント化されたメッセージには無効であることを示します。このパラメータが指定されていない場合は、このルールがフラグメント化されていないメッセージとフラグメント化されたメッセージの両方に対して有効であることを示します。

logging:該当するメッセージにログ情報を記録できることを示す。この機能では、ACL を使用するモジュールが、メッセージフィルタリングなどのロギング機能をサポートする必要があります。

source {source-address source-wildcard |any}:ルールの送信元 IP アドレス情報を指定します。source-address はメッセージの送信元 IP アドレス、source-wildcard は送信元 IP アドレスのワイルドカードマスク(ホストアドレスは 0 です。)、any は任意の送信元 IP アドレスを表します。

time-range time-range-name:この規則が有効になる期間を指定します。time-range-name は期間の名前です。1~32 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。期間が設定されていない場合、ルールは正常に作成されますが、プロンプトが表示され、期間の設定が完了するまでルールは有効になりません。期間の詳細と構成手順については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*2 章 タイムレンジ*”を参照してください。

説明

rule コマンドを使用して、IPv4 基本 ACL のルールを作成します。

undo rule コマンドを使用して、IPv4 基本 ACL のルールまたはルールの一部を削除します。

rule コマンドを使用して、番号を指定するルールが存在しない場合は、新しいルールを作成します。番号付けされた規則がすでに存在する場合は、古い規則が変更され、元の内容に新しい内容が追加されます。

新しく作成または変更されたルールは、既存のルールと同じ内容にすることはできません。同じ内容にすると、エラーが表示され、操作が失敗します。

ACL のルール一致順序が設定されている場合、ACL 内の既存のルールを変更できます。ACL のルール一致順序が自動ソートの場合、ACL 内の既存のルールを変更することはできません。変更しないと、エラーが表示されます。

display acl all コマンドは、既存のすべての IPv4 拡張 ACL ルールと IPv4 基本 ACL ルールを表示します。

ルールを削除する場合は、次の点に注意してください。

- **undo rule rule-id** コマンドを使用するときにオプションのパラメータを指定しないと、ルール全体が削除されます。オプションのパラメータが指定されている場合は、そのパラメータの内容のみが削除されます。
- **undo rule {deny |permit }**コマンドではルールの一部を削除できません。**undo rule {deny |permit }**コマンドを使用する場合は、既存のルールの完全な形式を入力する必要があります。

例

#IPv4 基本 ACL 2000 のルールを次のように作成します。10.0.0.0/8、172.17.0.0/16、および 192.168.1.0/24 ネットワークセグメントからのメッセージの通過のみを許可し、その他すべてのネットワークセグメントからのメッセージの通過を拒否します。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range (セキュリティ/タイムレンジ)**

1.1.8 rule (Layer 2 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **time-range**] *

undo rule { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

デフォルト

レイヤ 2 ACL にはルールがありません。

View

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id:レイヤ 2 ACL ルールの番号を 0~65534 の範囲で指定します。このパラメータが指定されていない場合、既存の最大数を超えるステップの最小倍数が、ルール番号の開始値から自動的に割り当てられます。たとえば、既存ルールの最大番号が 28,ステップサイズが 5 であれば、自動的に割り当てられる新しい番号は 30 となる。

deny:条件を満たすメッセージを拒否することを示す。

permit:条件を満たすメッセージを許可することを示す。

cos dot1p:802.1 p 優先度を指定します。dot1p は 802.1 p 優先度を表し、次の形式で入力できます。

- 数値:0~7 の範囲;
- 名前:best-effort、background、spare、excellent-effort、controlled-load、video、voice、network-management は、数字の 0~7 に対応します。

counting:ルール・マッチング・ソフトウェア統計がオンで、デフォルトでオフになっていることを示します。

dest-mac dest-address dest-mask:宛先 MAC アドレスの範囲を指定します。dest-address は宛先 MAC アドレスで、H-H-H の形式です。dest-mask は宛先 MAC アドレスのマスクを表し、H-H-H の形式になります。

lsap lsap-type lsap-type-mask:LLC カプセル化の DSAP フィールドと SSAP フィールドを指定します。lsap-type は、16 進数の 0~ffff の範囲でデータフレームをカプセル化する形式です。lsap-type-mask は、マスクビットを指定する LSAP のタイプマスクで、16 進数の 0~ffff の範囲で値を指定します。

type protocol-type protocol-type-mask:リンク層プロトコルタイプを指定します。protocol-type はデータフレームタイプで、Ethernet_II タイプと Ethernet_SNAP タイプのフレームの type フィールドに対応し、16 進数の 0~ffff の範囲の値を取ります。protocol-type-mask はマスクビットを指定するタイプマスクで、16 進数の 0~ffff の範囲で値を指定します。

source-mac source-address source-mask:送信元 MAC アドレスの範囲を指定します。source-address は、送信元 MAC アドレスを H-H-H の形式で表したものです。source-mask は、送信元 MAC アドレスのマスクを H-H-H の形式で表します。

time-range time-range-name:この規則が有効になる期間を指定します。time-range-name は期間の名前です。1~32 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。期間が設定されていない場合、ルールは正常に作成されますが、プロンプトが表示され、期間の設定が完了するまでルールは有効になりません。期間の詳細と構成手順については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*2 章 タイムレンジ*”を参照してください。

説明

rule コマンドを使用して、レイヤ 2 ACL のルールを作成します。

undo rule コマンドを使用して、レイヤ 2 ACL のルールまたはルールの一部を削除します。

rule コマンドを使用して、番号を指定するルールが存在しない場合は、新しいルールを作成します。番号付けされた規則がすでに存在する場合は、古い規則が変更され、元の内容に新しい内容が追加されます。

新しく作成または変更されたルールは、既存のルールと同じ内容にすることはできません。同じ内容にすると、エラーが表示され、操作が失敗します。

ACL のルール一致順序が設定されている場合、ACL 内の既存のルールを変更できます。ACL のルール一致順序が自動ソートの場合、ACL 内の既存のルールを変更することはできません。変更しないと、エラーが表示されます。

display acl mac all コマンドは、既存のすべてのレイヤ 2 ACL ルールを表示します。

ルールを削除する場合は、次の点に注意してください。

- **undo rule rule-id** コマンドを使用するときにオプションのパラメータを指定しないと、ルール全体が削除されます。オプションのパラメータが指定されている場合は、そのパラメータの内容のみが削除されます。
- **undo rule {deny |permit }**コマンドではルールの一部を削除できません。**undo rule {deny |permit }**コマンドを使用する場合は、既存のルールの完全な形式を入力する必要があります。

例

#レイヤ 2 ACL 4000 のルールを次のように作成します。ARP メッセージの通過は許可しますが、RARP メッセージの通過は拒否します。

<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000] rule permit type 0806 ffff
[Sysname-acl-mac-4000] rule deny type 8035 ffff

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range (セキュリティ/タイムレンジ)**

1.1.9 rule comment

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

デフォルト

ルールには情報が記述されていません。

View

IPv4 basic/advanced ACL view

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id:存在する必要があるルールの番号を指定します。範囲は 0~65534 です。

text:ルールの説明を示す 1~127 文字の文字列で、大文字と小文字が区別されます。

説明

rule comment コマンドを使用して、ルールの説明情報を設定します。

undo rule comment コマンドを使用して、指定したルールの説明情報を削除します。

rule comment コマンドを使用すると、指定したルールに記述情報がない場合はそのルールに記述情報が追加され、それ以外の場合は変更されます。

例

#IPv4 基本 ACL 2000 のルール 0 を設定し、そのルールの説明情報を設定します。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on gigabitethernet 1/0/1.
```

関連コマンド

- **display acl**

1.1.10 step

Syntax

step *step-value* [**start** *start-value*]

undo step

デフォルト

ルール番号のステップサイズは 5 で、開始値は 5 です。

View

IPv4 basic/advanced ACL view

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

step-value:ルール番号を表すステップ値。範囲は 1~20 です。

start-value:ルール番号の開始値を示します。範囲は 0~20 です。

説明

step コマンドは、ルール番号のステップサイズを設定します。

undo step コマンドを使用して、デフォルトの状態を復元します。

ルールに番号が自動的に割り当てられる方法は、次のとおりです。既存の最大番号を超えるステップの最小倍数が、ルール番号の開始値から自動的に割り当てられます。たとえば、番号が 0、5、9、10、12 の 5 つの規則があり、ステップサイズが 5 の場合、番号を指定せずに規則を作成すると、自動的に番号 15 が割り当てられます。

ステップサイズまたはルール番号の開始値が変更されると、ACL 内の元のすべてのルールの番号が、ルール番号の開始値からステップごとに自動的に再配置されます。たとえば、ある ACL 内には 0, 5, 9, 10, 15 という番号の 5 つのルールがあったが、ステップサイズを 2 に変更すると、それらのルールの番号は 5, 7, 9, 11, 13 となる。

例

#IPv4 ベース ACL 2000 のルール番号のステップサイズを 2 に設定します。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] step 2
```

関連コマンド

- **display acl**

目次

このセクションのページは **15-x-x** です。

2 章 Packet filter 2-1
2.1 Packet filter 設定コマンド 2-1
2.1.1 packet-filter (interface view) 2-1
2.1.2 packet-filter (service template view) 2-2

2章 Packet filter

2.1 Packet filter 設定コマンド

2.1.1 packet-filter (interface view)

Syntax

packet-filter [**mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

undo packet-filter [**mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

mac: レイヤ 2 ACL タイプを指定します。

acl-number: ACL を番号で指定します。使用可能な値の範囲は次のとおりです。

- 2000～2999 : 標準 IPv4 ACL です。
- 3000～3999 : 拡張 IPv4 ACL です。
- 4000～4999 : L2 ACL です。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 文字で、大文字と小文字を区別しません。

inbound: 受信パケットをフィルタリングします。

outbound: 送信パケットをフィルタリングします。

説明

packet-filter コマンドは、インタフェースに ACL を適用します。

undo packet-filter コマンドは、インタフェースから ACL を削除します。

ACL の **rule** コマンドの **counting** キーワードは、ルールに固有の一致カウントを有効にします。

インタフェースの同じ方向に対して、最大 32 個の ACL を適用できます。

例

GigabitEthernet 1/0/1 に対し、受信したトラフィックをフィルタリングするため、IPv4 標準 ACL 2001 を適用します。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] packet-filter 2001 inbound

2.1.2 packet-filter (service template view)

Syntax

packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

undo packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

acl-number: ACL を番号で指定します。使用可能な値の範囲は次のとおりです。

- 2000～2999 : 標準 IPv4 ACL です。
- 3000～3999 : 拡張 IPv4 ACL です。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 文字で、大文字と小文字を区別しません。

inbound: 受信パケットをフィルタリングします。

outbound: 送信パケットをフィルタリングします。

説明

packet-filter コマンドは、サービステンプレートに ACL を適用します。

undo packet-filter コマンドは、サービステンプレートから ACL を削除します。

サービステンプレートのパケットをフィルタリングするには、AC でサービステンプレートに ACL を適用し、AP で適用 ACL を作成する必要があります。

サービステンプレートに適用できる ACL は、送信元 IP アドレス、宛先 IP アドレス、送信元ポート番号、宛先ポート番号、およびパケットのプロトコルだけです。

サービステンプレートの同一方向に適用できる ACL は 1 つだけです。

サービステンプレートが無効の場合だけ設定変更できます。

例

サービステンプレート service1 に対し、受信したトラフィックをフィルタリングするため、IPv4 標準 ACL 2001 を適用します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] packet-filter 2001 inbound

目次

このセクションのページは **15-x-x** です。

3 章 タイムレンジ 3-1
3.1 タイムレンジ設定コマンド 3-1
3.1.1 display time-range 3-1
3.1.2 time-range 3-2

3章 タイムレンジ

3.1 タイムレンジ設定コマンド

3.1.1 display time-range

Syntax

display time-range { *time-range-name* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

time-range-name:指定した名前期間の構成およびステータス情報を表示します。time-range-name は期間の名前です。1~32 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。

all:すべての期間の構成およびステータス情報を表示します。

説明

display time-range コマンドは、期間の設定情報とステータス情報を表示します。

例

#期間 t 4 の構成およびステータス情報を表示します。

<Sysname> display time-range t4

```
Current time is 17:12:34 11/23/2019 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2019 to 00:00 1/1/2020
 from 00:00 6/1/2019 to 00:00 7/1/2019
```

表 3-1 display time-range コマンドの表示情報の説明

フィールド	説明
Current time	システムの現在の時刻

フィールド	説明
Time-range	期間の構成情報。次の情報が含まれます。 • 期間の名前 • 期間のステータス。Active (発効)とInactive (未発効)の2つのステータスがあります。 • 期間の時間範囲

3.1.2 time-range

Syntax

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

デフォルト

期間がありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

time-range-name:期間の名前を 1~32 文字の文字列で指定します。大文字と小文字は区別されず、a~z または A~Z で始まる必要があります。混乱を避けるため、期間の名前に英語の all を使用することはできません。

start-time to end-time:期間の時間範囲を指定します。start-time は開始時間で、フォーマットは hh:mm、範囲は 00:00~23:59 です。end-time は終了時間を表します。hh:mm の形式で 00:00~24:00 の値を取り、終了時間は開始時間よりも大きくする必要があります。

days:サイクルタイムが有効になる曜日を指定します。このパラメータは複数回入力できますが、後から入力した値は前に入力した値と完全に重なることはできず(たとえば 6 を入力した後に Sat を再入力することは許されないが、再入力は許される off-day)、システムは各入力値の和を最終値として取ります(たとえば、 1, Wed, working-day の順に入力すると、最終的に有効になるのは 1 週間の勤務日である)。このパラメータは次の形式で入力できます。

- 数値:日~土の順に 0~6 の範囲で指定します。
- 曜日の英語略称(日曜日から土曜日まで、Sun、Mon、Tue、Wed、Thu、Fri、Sat);
- 平日(working-day):月曜日から金曜日;

- 休日(off-day):土曜日と日曜日を示します。
- (daily):週 7 日を表します。

from time1 date1:絶対期間の開始時間を指定します。time1 のフォーマットは hh:mm で、00:00~23:59 の範囲で値を指定できます。date1 の形式は MM/DD/YYYY または YYYY/MM/DD です。MM は月を表し、値の範囲は 1~12 です。DD は日を表し、入力した月に応じて値が変わります。YYYY は年を表し、1970~2100 の値を取ります。このパラメータを指定しない場合、絶対期間の開始時刻は、システムが表示できる最も早い時刻である 1970 年 1 月 1 日 0:00 になります。

to time2 date2:絶対期間の終了時刻を指定します。time2 のフォーマットは hh:mm で、00:00~24:00 の範囲で値を指定できます。date2 の形式は MM/DD/YYYY または YYYY/MM/DD です。MM は月を表し、値の範囲は 1~12 です。DD は日を表し、入力した月に応じて値が変わります。YYYY は年を表し、1970~2100 の値を取ります。終了時間は開始時間より大きくなければなりません。このパラメータが指定されていない場合、絶対期間の終了時刻は、システムが表示できる最も遅い時刻である 2100 年 12 月 31 日 24:00 になります。

説明

time-range コマンドは、特定の時間範囲を表す期間を作成します。このコマンドは、指定した期間がすでに作成されている場合に、期間の時間範囲を変更します。

undo time-range コマンドは、期間を削除するために使用します。

指定した名前の期間が存在しない場合は、新しい期間を作成します(最大 1024)。指定した名前の期間がすでに存在する場合は、古い期間が変更され、元のコンテンツに新しいコンテンツが追加されます。

期間では、次の 2 つの方法で時間範囲を定義できます。

- start-time to end-time days パラメータセットを使用して作成された期間は、1 週間単位で有効になる期間です。
- from time1 date1 および to time2 date2 パラメータのセットを使用して作成される期間は、指定した期間内に有効になる絶対期間です。

1 つの期間に両方の時間範囲が含まれている場合は、期間期間と絶対期間の交差を有効な時間範囲とします。たとえば、サイクルタイムを毎週月曜日の 8 時から 12 時まで、絶対タイムを 2019 年通年までと定義すると、タイムゾーンは 2019 年通年で毎週月曜日の 8 時から 12 時まで有効です。

1 つの期間は、1 つまたは複数の周期的期間(最大 32)および絶対的期間(最大 12)を含むことができ、複数の周期的期間および絶対的期間を含む場合、システムは、各周期的期間の和集合および各絶対的期間の和集合をそれぞれ取得し、2 つの和集合の交差を、期間が最終的に有効になる時間範囲として取得する。

例

#毎週の平日の 8 時から 18 時までの t 1 という時間枠を作成します。

<Sysname> system-view

[Sysname] time-range t1 08:00 to 18:00 working-day

#t 2 という名前の期間を作成します。期間は 2019 年の 1 年間です。

<Sysname> system-view

[Sysname] time-range t2 from 00:00 1/1/2019 to 24:00 12/31/2019

#2019 年の年中無休の 8 時から 12 時までの t 3 というタイムゾーンを作成します。

<Sysname> system-view

[Sysname] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2019 to 24:00 12/31/2019

#2019 年 1 月と 6 月に、毎週月曜日の 10 時から 12 時までと毎週水曜日の 14 から 16 時までの t 4 という時間枠を作成します。

<Sysname> system-view

[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2019 to 24:00 1/31/2019

[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2019 to 24:00 6/30/2019

関連コマンド

- **display time-range**

目次

このセクションのページは **15-x-x** です。

4 章 パスワード管理 4-1
4.1 パスワード管理設定コマンド 4-1
4.1.1 display password-control 4-1
4.1.2 display password-control blacklist 4-3
4.1.3 password-control { aging | composition | history | length } enable 4-4
4.1.4 password-control aging 4-6
4.1.5 password-control alert-before-expire 4-8
4.1.6 password-control authentication-timeout 4-8
4.1.7 password-control blacklist all-line 4-9
4.1.8 password-control change-password first-login enable 4-10
4.1.9 password-control change-password weak-password enable 4-11
4.1.10 password-control complexity 4-12
4.1.11 password-control composition 4-14
4.1.12 password-control enable 4-15
4.1.13 password-control expired-user-login 4-17
4.1.14 password-control history 4-18
4.1.15 password-control length 4-19
4.1.16 password-control login idle-time 4-20
4.1.17 password-control login-attempt 4-21
4.1.18 password-control super aging 4-23
4.1.19 password-control super composition 4-24
4.1.20 password-control super length 4-25
4.1.21 password-control update-interval 4-26
4.1.22 reset password-control blacklist 4-27
4.1.23 reset password-control history-record 4-27

4章 パスワード管理

4.1 パスワード管理設定コマンド

4.1.1 display password-control

Syntax

display password-control [**super**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

super:super パスワード管理の設定情報を表示します。このパラメータを指定しない場合は、グローバルパスワード管理の構成情報が表示されます。

説明

display password-control コマンドは、パスワード管理の設定情報を表示します。

例

#グローバルパスワード管理の構成情報を表示します。

<Sysname> display password-control

```
Global password control configurations:
Password control:Enabled
Password aging:Enabled (90 days)
Password length:Enabled (10 characters)
Password composition:Enabled (1 types、1 characters per type)
Password history:Enabled (max history records:4)
Early notice on password expiration:7 days
Maximum login attempts:3
Action for exceeding login attempts:Lock user for 1 minutes
Password history was last reset:0 days ago
Minimum interval between two updates:24 hours
User account idle time:90 days
Logins with aged password:3 times in 30 days
Password complexity:Disabled (username checking)
```

```
Disabled (repeated characters checking)
Password change:Enabled (first login)
Enabled (mandatory weak password change)
```

#super パスワード管理の設定情報を表示します。

<Sysname> display password-control super

```
Super password control configurations:
Password aging:Enabled (90 days)
Password length:Enabled (10 characters)
Password composition:Enabled (1 types、1 characters per type)
```

表 4-1 display password-control コマンドの表示情報の説明

フィールド	説明
Global password control configurations	グローバルパスワード管理構成
Super password control configurations	Superパスワード管理の設定
Password control	グローバルパスワード管理機能のオン状態
Password aging	パスワードエージング機能のオン状態(パスワードのエージングタイム)
Password length	パスワード最小長機能がオンになっている状態(パスワードの最小長)
Password composition	パスワードの組み合わせポリシーが有効になっている(パスワード要素の組み合わせのタイプ、少なくとも各要素の数)
Password history	パスワード履歴機能のオン状態(パスワード履歴の最大数)
Early notice on password expiration	パスワードが期限切れになるまでのリマインダ時間
Maximum login attempts	ユーザの最大ログイン試行回数
Action for exceeding login attempts	ログイン試行回数が設定回数に達した後のユーザーアカウントのロック動作
Password history was last reset	ユーザのパスワード履歴が最後に消去された時刻
Minimum interval between two updates	パスワード更新の最小間隔
User account idle time	ユーザーアカウントアイドル時間
Logins with aged password	パスワードが期限切れになってからユーザがログインできるようになった回数と時間
Password complexity	パスワードの複雑度チェック機能がオンになっている(ユーザ名が含まれているかどうか、またはユーザ名が逆になっているかどうかを確認します;同じ文字が3つ以上含まれているかどうかを確認します)

フィールド	説明
Password change	初回ログインパスワード変更機能のステータス: • Enabled (first login):初回ログイン時のパスワード変更機能を有効にする • Disabled (first login):初回ログイン時のパスワード変更機能をオフにする • Enabled (mandatory weak password change):弱いパスワードのログイン強制暗号化機能を有効にする • Disabled (mandatory weak password change):弱いパスワードによるログイン強制暗号化を無効にする

4.1.2 display password-control blacklist

Syntax

display password-control blacklist [**user-name** *user-name* | **ip** *ipv4-address* | **ipv6** *ipv6-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-name user-name:パスワード管理ブラックリストに指定されたユーザ名のユーザ情報を表示します。ここで、user-name はユーザ名を表します。は 1~80 文字の文字列で、大文字と小文字が区別されます。

ip ipv4-address:パスワード管理ブラックリストに指定された IPv 4 アドレスのユーザ情報を表示します。

ipv6 ipv6-address:パスワード管理ブラックリストに指定された IPv 6 アドレスのユーザ情報を表示します。

説明

display password-control blacklist コマンドは、ユーザ認証が失敗した後にパスワード管理ブラックリストに追加されたユーザ情報を表示します。

パラメータを指定しない場合は、パスワード管理ブラックリスト内のすべてのユーザ情報が表示されます。

ユーザが認証に失敗すると、IP アドレスとユーザ名がパスワード管理のブラックリストに追加されます。このコマンドを使用すると、パスワード管理ブラックリストに登録されている FTP ユーザと、Web または VTY 経由でデバイスにアクセスするユーザを表示できます。

Console ポートを介してアプライアンスに接続されているユーザは、システムから IP アドレスを取得できません。また、アプライアンスにアクセスするユーザはすでにある程度の権限とセキュリティを持っているため、認証に失敗してもパスワード管理のブラックリストに登録されません。

例

#ユーザ認証に失敗した後、パスワード管理ブラックリストに登録されたユーザの情報を表示する。

<Sysname> display password-control blacklist

```
Blacklist items matched: 2.
Username                  IP address          Login failures   Lock flag
 abcd                     169::168:34:1        4               lock
 admin                    192.168.34.1         1               unlock
```

表 4-2　display password-control blacklist コマンドの表示情報の説明

フィールド	説明
Blacklist items matched	一致するブラックリストテーブルエントリの数
Username	ユーザ名
IP address	ユーザのIPアドレス
Login failures	ユーザのログインに失敗した回数
Lock flag	ユーザがロックされているかどうか • unlock:ロックされていないため、ユーザはログインを再試行できます。 • lock:ログインに失敗した IP アドレスを使用してユーザがログインを試行できないように一時的または永続的にロックされていることを示します(具体的には password-control login-attempt コマンドの構成によって決定される.)。

4.1.3 password-control { aging | composition | history | length } enable

Syntax

password-control { aging | composition | history | length } enable

undo password-control { aging | composition | history | length } enable

デフォルト

各パスワード管理機能はオンになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

aging:パスワードエージング管理機能を有効にします。

composition:パスワードの組み合わせ検出管理機能を有効にします。

history:パスワード履歴検出管理機能を有効にします。

length:パスワードの最小長管理機能を有効にします。

説明

password-control {aging |composition |history |length } enable コマンドは、指定したパスワード管理機能を有効にします。

undo password-control {aging |composition |history |length } enable コマンドを使用して、指定したパスワード管理機能を無効にします。

パスワードエージング管理機能とパスワード履歴検出管理機能を有効にするには、まずグローバルパスワード管理機能を有効にし、次にパスワードエージング管理機能または履歴検出管理機能を有効にする必要があります。

非 FIPS モードでは、パスワードの組み合わせ検出管理機能とパスワード最小長管理機能がデフォルトでオンになっており、グローバルパスワード管理機能がオンになっているかどうかには依存しません。デフォルトでは、パスワードの最小長とパスワードに含まれる要素の組み合わせの制限はデバイスのモデルに依存します。デバイスの実際の状況に基づいてください。

デバイス管理クラスのローカルユーザのパスワードを HASH モードで設定すると、グローバルおよび指定のパスワード管理機能がオンになっていても、パスワードの長さ、組み合わせポリシー、複雑さはチェックされず、すべての記録された履歴パスワードおよび現在のパスワードと比較されません。デバイス管理クラスのローカルユーザパスワードの構成方法については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*13 ユーザアクセスと認証*“の”*3 章 AAA*“を参照してください。

パスワード履歴管理機能をオフにすると、システムは新しいパスワードがすべての履歴パスワードと異なるかどうかを検出しなくなりますが、履歴パスワード履歴機能はオフになりません。記録されたユーザの履歴パスワードの数が **password-control history max-record-number** コマンドで設定された最大数に達すると、そのユーザの以降の新しいパスワード履歴が最も古いパスワード履歴を上書きします。

例

#グローバルパスワード管理機能を有効にする。

<Sysname> system-view

[Sysname] password-control enable

#パスフレーズ検出管理機能を有効にする。

[Sysname] password-control composition enable

#パスワードエージング機能をオンにします。

[Sysname] password-control aging enable

#パスワードの最小長機能を有効にします。

[Sysname] password-control length enable

#パスワード履歴機能を有効にする。

[Sysname] password-control history enable

関連コマンド

- **display password-control**
- **password-control enable**

4.1.4 password-control aging

Syntax

password-control aging *aging-time*

undo password-control aging

デフォルト

グローバルなパスワードエージング時間は 90 日;ユーザグループのパスワードエージング時間グローバルに設定されたパスワードエージング時間;ローカルユーザのパスワードエージング時間は、所属ユーザグループのパスワードエージング時間です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

aging-time:パスワードのエージングタイム。1~365 の範囲で、単位は日です。

説明

password-control aging コマンドを使用して、パスワードのエージングタイムを設定します。

undo password-control aging コマンドを使用して、デフォルトの状態を復元します。

エージングタイムはビューによって異なります。

- システムビューの時間はグローバルな意味を持ち、すべてのユーザグループに適用されます。
- ユーザグループビューの時間は、ユーザグループ内のすべてのローカルユーザに適用されます。
- ローカルユーザービューの時間は、ローカルユーザにのみ適用されます。

アプリケーションスコープが小さいパスワードのエージングタイムの方が高優先となります。システムは、ローカルユーザのローカルユーザービューでのパスワードエージングタイムを優先して使用します。

- ローカルユーザにパスワードエージングタイムが設定されていない場合、システムはローカルユーザが属するユーザグループのパスワードエージングタイムを使用します。
- ユーザグループにパスワードエージングタイムが設定されていない場合、システムはグローバルパスワードエージングタイムを使用します。

例

#グローバルなパスワードエージング時間を 80 日に設定します。

<Sysname> system-view

[Sysname] password-control aging 80

#ユーザグループ test のためのパスワードエージングタイムを 90 日設定して下さい。

[Sysname] user-group test

[Sysname-ugroup-test] password-control aging 90

[Sysname-ugroup-test] quit

#設定デバイス管理クラスローカルユーザ abc のためのパスワードエージングタイムは 100 日です。

[Sysname] local-user abc class manage

[Sysname-luser-manage-abc] password-control aging 100

関連コマンド

- **display local-user (ユーザアクセスと認証/AAA)**
- **display password-control**
- **display user-group (ユーザアクセスと認証/AAA)**
- **password-control aging enable**

4.1.5 password-control alert-before-expire

Syntax

password-control alert-before-expire alert-time

undo password-control alert-before-expire

デフォルト

パスワードの有効期限が切れるまでのリマインダ期間は 7 日間です。これは、ユーザがログインしたときに、パスワードの有効期限が切れることをユーザに通知するためです。

View

System view

定義済みユーザロール

network-admin

パラメータ

alert-time:パスワードの有効期限が切れるまでのリマインダ時間。1~30 日の範囲で指定できます。

説明

password-control alert-before-expire コマンドは、パスワードが期限切れになるまでのアラーム時間を設定します。

undo password-control alert-before-expire コマンドを使用して、デフォルトの状態を復元します。

FTP ユーザがパスワードを変更することは許可されておらず、管理者が変更できるのは FTP ユーザのパスワードだけなので、このコマンドで設定されている有効期限アラームは、FTP タイプ以外の Login ユーザに対してのみ有効です。

例

#パスワードの有効期限が切れるまでのリマインダを 10 日に設定します。

<Sysname> system-view

[Sysname] password-control alert-before-expire 10

関連コマンド

- **display password-control**

4.1.6 password-control authentication-timeout

Syntax

password-control authentication-timeout *timeout*

undo password-control authentication-timeout

デフォルト

600 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

timeout:ユーザ認証タイムアウト時間を秒単位で 30 から 600 の範囲で指定します。

説明

password-control authentication-timeout コマンドを使用して、ユーザ認証タイムアウト時間を設定します。

デフォルトに戻すには、**undo password-control authentication-timeout** コマンドを使用します。

このコマンドは、Telnet およびターミナルユーザに対してのみ有効です。ユーザの認証がタイムアウトすると、接続は終了します。

例

#ユーザ認証タイムアウト時間を 40 秒に設定します。

<Sysname> system-view

[Sysname] password-control authentication-timeout 40

関連コマンド

- **display password-control**

4.1.7 password-control blacklist all-line

Syntax

password-control blacklist all-line

undo password-control blacklist all-line

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

すべてのユーザ回線タイプに対してパスワード制御ブラックリスト機能を有効にするには、**password-control blacklist all-line** コマンドを使用します。
すべてのユーザ回線タイプに対してパスワード制御ブラックリスト機能を無効にするには、**undo password-control blacklist all-line** を使用します。
デフォルトでは、グローバルパスワード制御機能を有効にすると、FTP、Web、および VTY ユーザに対してのみパスワード制御ブラックリスト機能が有効になります。すべての AUX ユーザ回線でログインユーザに対してパスワード制御ブラックリスト機能を有効にするには、このコマンドも実行する必要があります。ユーザ回線の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*3 章 ログイン管理*”を参照してください。
この機能を有効にすると、AUX ユーザについて、同じユーザアカウントでの連続ログイン失敗回数が累積されます。この回数が上限に達すると、システムはそのユーザアカウントをブラックリストに追加し、対応するアクションを実行します。
パスワード制御ログイン試行を使用して、連続ログイン失敗の最大回数と、最大回数に達したときのアクションを設定します。

例

#すべてのユーザ回線タイプに対してパスワード制御ブラックリスト機能を有効にします。

<Sysname> system-view

[Sysname] password-control blacklist all-line

関連コマンド

- **display password-control**
- **display password-control blacklist**
- **password-control enable**
- **password-control login-attempt**

4.1.8 password-control change-password first-login enable

Syntax

password-control change-password first-login enable

undo password-control change-password first-login enable

デフォルト

ユーザが初めてデバイスにログインしたときにパスワードを変更する機能がオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

password-control change-password first-login enable コマンドを使用すると、初回ログイン時にパスワードを変更できます。

undo password-control change-password first-login enable コマンドを使用すると、初回ログイン時のパスワード変更機能が無効になります。

初回ログイン時のパスワード変更機能を有効にするには、グローバルパスワード管理機能と初回ログイン時のパスワード変更機能の両方がオンになっている必要があります。

例

#初回ログイン時のパスワード変更機能を有効にする。

<Sysname> system-view
[Sysname] password-control change-password first-login enable

関連コマンド

- **display password-control**
- **password-control enable**

4.1.9 password-control change-password weak-password enable

Syntax

password-control change-password weak-password enable

undo password-control change-password weak-password enable

デフォルト

弱いパスワードによるログインパスワードの変更機能が無効になっています。

View

System view

定義済みユーザロール

network-admin

説明

password-control change-password weak-password enable コマンドを使用して、弱いパスワードログインを有効にし、パスワード機能を変更します。

undo password-control change-password weak-password enable コマンドを使用して、弱いパスワードログインパスワードの変更機能を無効にします。

Telnet、SSH、HTTP、HTTPS 方式でログインする設備管理類ユーザは、ログインパスワードを入力する時、システムは現在設定された Password control パスワードの組み合わせ検出策略、パスワードの最小長さ制限及びパスワード複雑度検査策略によってユーザのログインパスワードを検査し、もし以上のパスワード検査策略の要求に符合しなければ、弱いパスワードと見なす。

デフォルトでは、弱いパスワードによるログインパスワードの変更機能はオフになっています。ユーザが弱いパスワードでデバイスにログインすると、メッセージが出力されますが、ユーザにパスワードの変更を強制することはありません。弱いパスワードでもデバイスにログインできます。デバイス使用の安全性を高めるために、このコマンドを設定することによって、Telnet、SSH、HTTP、HTTPS 方式でログインするデバイス管理クラスのユーザが弱いパスワードでログインすることを禁止できます。アプライアンスは、パスワードの組み合わせポリシー、パスワードの長さ、パスワードの複雑性チェックポリシーの設定がアプライアンスの要件を満たすまで、弱いパスワードのログインユーザーにパスワードの変更を要求します。

現在のパスワード設定要件は、**display password-control** コマンドを使用して確認できます。また、**password-control composition**、**password-control length**、および **password-control complexity** コマンドを使用して、パスワードの組み合わせポリシー、パスワードの長さ、およびパスワードの複雑性チェックポリシーの設定を変更できます。

例

#System view で、弱いパスワードのログインパスワードの変更機能を有効にします。

<Sysname> system-view
[Sysname] password-control change-password weak-password enable

関連コマンド

- **display password-control**
- **password-control {aging |composition |history |length } enable**
- **password-control complexity**
- **password-control composition**
- **password-control length**
- **password-control enable**

4.1.10 password-control complexity

Syntax

password-control complexity {same-character |user-name } check

undo password-control complexity {same-character |user-name } check

デフォルト

グローバルパスワード複雑度チェックポリシーは、ユーザパスワードの複雑度をチェックします。ユーザ名または文字の順序が逆のユーザ名をパスワードに含めることはできませんが、同じ文字を 3 つ以上連続して含めることはできます。ユーザグループのパスワード複雑度チェックポリシーグローバルパスワード複雑度チェックポリシー;ローカルユーザのパスワード複雑度チェックポリシー所属ユーザグループのパスワード複雑度チェックポリシー。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

same-character:パスワードに同じ文字が 3 つ以上連続して含まれているかどうかをチェックするように指定します。たとえば、パスワード aaabc はこの複雑度チェックには該当しません。

user-name:パスワードにユーザ名が含まれているかどうかをチェックするユーザ名を指定します。たとえば、ユーザ名が 123 の場合、パスワード abc123、321 df はこの複雑度チェックに一致しません。

説明

password-control complexity コマンドを使用して、ユーザパスワードの複雑度チェックポリシーを設定します。

undo password-control complexity コマンドは、指定されたパスワード複雑度チェックポリシーをキャンセルするために使用します。

System view の下の構成はグローバルで、すべてのユーザグループに対して有効であり、User group view の下の構成はユーザグループ内のすべてのローカルユーザに対して有効であり、ローカル User view の下の構成は現在のローカルユーザに対してのみ有効です。

構成が有効になる優先度は、 「ローカルユーザ」 、 「ユーザグループ」 、 「グローバル」 の順になります。すなわち、システムはローカル User view での配置を優先し、ローカル User view で配置されていなければ User group view での配置を採用し、User group view でも配置されていなければグローバルビューでの配置を採用する。

ユーザ名がパスワードに含まれているかどうかを確認したり、ユーザ名の文字の順序が逆になっているかどうかを確認したりする機能は、グローバルパスワード管理機能がオンになっているかどうかには依存しません。

このコマンドを複数回実行すると、連続文字チェック機能だけでなく、ユーザ名チェック機能もオンにできます。

例

#パスワードの複雑さの検出ポリシーを設定するには、設定したパスワードにユーザ名が含まれているかどうか、または文字の順序が逆のユーザ名が含まれているかどうかを確認します。

<Sysname> system-view
[Sysname] password-control complexity user-name check

関連コマンド

- **display local-user (ユーザアクセスと認証/AAA)**
- **display password-control**
- **display user-group (ユーザアクセスと認証/AAA)**

4.1.11 password-control composition

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

デフォルト

グローバルのパスワード構成ポリシーは、少なくとも 2 種類の文字タイプと、各タイプに 1 文字以上を含む必要があります。

ユーザグループのパスワード構成ポリシーはグローバルの設定と同一です。ローカルユーザのパスワード構成ポリシーはローカルユーザが所属しているユーザグループのパスワード構成ポリシーと同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

type-number type-number:パスワード要素の最小組み合わせタイプ。ここで、type-number は組合せタイプの数を表し、1~4 の値を取ります。

type-length type-length:パスワードに含まれる要素の数。ここで、type-length は要素の数を表し、1~63 の値を取ります。

説明

password-control composition コマンドを使用して、ユーザパスワードの組み合わせポリシーを設定します。

undo password-control composition コマンドを使用して、デフォルトの状態を復元します。

System view の下の構成はグローバルで、すべてのユーザグループに対して有効であり、User group view の下の構成はユーザグループ内のすべてのローカルユーザに対して有効であり、ローカル User view の下の構成は現在のローカルユーザに対してのみ有効です。

構成が有効になる優先度は、 「ローカルユーザ」 、 「ユーザグループ」 、 「グローバル」 の順になります。すなわち、システムはローカル User view での配置を優先し、ローカル User view で配置されていなければ User group view での配置を採用し、User group view でも配置されていなければグローバルビューでの配置を採用する。

パスワード要素の最小の組み合わせタイプの数と各要素の最小数の積は、パスワードの最大長を超えることはできません。

例

#設定グローバルなパスワード要素の最小組み合わせタイプは 4 つで、各要素の数は 5 つ以上です。

<Sysname> system-view
[Sysname] password-control composition type-number 4 type-length 5

#ユーザグループ test を構成するパスワード要素の最小組み合わせタイプは 4 つで、各要素の数は 5 つ以上です。

[Sysname] user-group test
[Sysname-ugroup-test] password-control composition type-number 4 type-length 5
[Sysname-ugroup-test] quit

#デバイス管理クラスの設定ローカルユーザ abc のパスワード要素の最小組み合わせタイプは 4 つで、各要素の数は少なくとも 5 つです。

[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control composition type-number 4 type-length 5

関連コマンド

- **display local-user (ユーザアクセスと認証/AAA)**
- **display password-control**
- **display user-group (ユーザアクセスと認証/AAA)**
- **password-control composition enable**

4.1.12 password-control enable

Syntax

password-control enable

undo password-control enable

デフォルト

グローバルパスワード管理機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

password-control enable コマンドは、グローバルパスワード管理機能を有効にします。

undo password-control enable コマンドを使用して、グローバルパスワード管理機能を無効にします。

パスワードの組み合わせ検出管理機能、パスワード最小長管理機能、およびパスワードにユーザ名が含まれているかどうかをチェックする機能、または文字の順序が逆であるユーザ名機能は、グローバルパスワード管理機能がオンであるかどうかに依存せず、他の指定されたパスワード管理機能は、グローバルパスワード管理機能が有効である場合にのみ有効である。

グローバルパスワード管理が有効になっている場合、デバイス管理クラスのローカルユーザのパスワードと super のパスワードの構成は表示されません。つまり、対応する displayコマンドを使用して、デバイス管理クラスのローカルユーザのパスワードと super のパスワードの構成を表示することはできません。ネットワークアクセスクラスのローカルユーザのパスワードは、パスワード管理機能によって制御されず、その設定表示も影響を受けません。

グローバルパスワード管理が有効になっている場合、最初に設定するデバイス管理クラスのローカルユーザパスワードは、少なくとも 4 つの異なる文字で構成する必要があります。

グローバルパスワード管理機能をオンにすると、「dat」というサフィックスが付いたファイルが自動的に生成され、ローカルユーザの認証・ログイン情報を記録するためにストレージメディアに保存されます。手動でファイルを削除または変更しないでください。

例

#グローバルパスワード管理機能を有効にする。

<Sysname> system-view
[Sysname] password-control enable

関連コマンド

- **display password-control**
- **password-control {aging |composition |history |length } enable**

4.1.13 password-control expired-user-login

Syntax

password-control expired-user-login delay *delay* **times** *times*

undo password-control expired-user-login

デフォルト

パスワードの有効期限が切れた後、ログインが許可される時間は 30 日で、ログインが許可される回数は 3 回です。つまり、パスワードの有効期限が切れた後、システムはユーザに古いパスワードで 30 日以内に 3 回のログインを許可します。30 日を超えた後、またはログイン回数が 3 回を超えた後、ユーザは新しいパスワードを設定するよう求められます。

View

System view

定義済みユーザロール

network-admin

パラメータ

delay *delay*:パスワードの有効期限が切れてからユーザがログインできるようになるまでの時間。1~90 日の範囲で指定できます。

times *times*:パスワードの有効期限が切れた後にユーザがログインできる最大回数。0~10 の値を指定します。0 を指定すると、パスワードの有効期限が切れると、ユーザは新しいパスワードを設定するように直接求められます。

説明

password-control expired-user-login コマンドを使用して、パスワードの有効期限が切れた後にユーザがログインできる時間と回数を設定します。

undo password-control expired-user-login コマンドを使用して、デフォルトの状態を復元します。

この設定は、FTP タイプ以外の Login ユーザにのみ有効です。FTP ユーザの場合、パスワードの有効期限が切れると、システムはログインを続行できません。

例

#パスワードの有効期限が切れてから 60 日以内に 5 回ログインできるように設定します。

<Sysname> system-view
[Sysname] password-control expired-user-login delay 60 times 5

関連コマンド

- **display password-control**

4.1.14 password-control history

Syntax

password-control history *max-record-number*

undo password-control history

デフォルト

ユーザごとのパスワード履歴の最大数は 4 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

max-record-number:ユーザパスワード履歴ごとの最大エントリ数。2~15 の値をとります。

説明

password-control history コマンドを使用して、ユーザごとのパスワード履歴の最大数を設定します。

undo password-control history コマンドを使用して、デフォルトの状態を復元します。

グローバルパスワード管理を有効にすると、履歴パスワードが継続的に記録されます。記録されたユーザのパスワード履歴が最大数に達すると、そのユーザの新しいパスワード履歴が最も古いパスワード履歴を上書きします。

パスワード履歴は、グローバルパスワード管理機能をオフにした場合(undo password-control enable)、またはパスワード履歴を手動でクリアした場合(reset password-control history-record)にのみクリアされます。

例

#ユーザごとのパスワード履歴の最大数を 10 個に設定します。

<Sysname> system-view
[Sysname] password-control history 10

関連コマンド

- **display password-control**
- **password-control history enable**
- **reset password-control blacklist**

4.1.15 password-control length

Syntax

password-control length *length*

undo password-control length

デフォルト

グローバルの最小パスワード長は 10 文字です。

ユーザグループの最小パスワード長はグローバルの設定と同一です。ローカルユーザの最小パスワード長はローカルユーザが所属しているユーザグループの最小パスワード長と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

length:パスワードの最小長。範囲は 4~32 です。

説明

password-control length コマンドを使用して、パスワードの最小長を設定します。

undo password-control length コマンドを使用して、デフォルトの状態を復元します。

System view の下の構成はグローバルで、すべてのユーザグループに対して有効であり、User group view の下の構成はユーザグループ内のすべてのローカルユーザに対して有効であり、ローカル User view の下の構成は現在のローカルユーザに対してのみ有効です。

構成が有効になる優先度は、 「ローカルユーザ」 、 「ユーザグループ」 、 「グローバル」 の順になります。すなわち、システムはローカル User view での配置を優先し、ローカル User view で配置されていなければ User group view での配置を採用し、User group view でも配置されていなければグローバルビューでの配置を採用する。

例

#グローバルパスワードの設定最小長は 16 文字です。

<Sysname> system-view
[Sysname] password-control length 16

#ユーザグループ test のパスワードを 16 文字以内で設定します。

[Sysname] user-group test

[Sysname-ugroup-test] password-control length 16
[Sysname-ugroup-test] quit

#デバイス管理クラスの設定ローカルユーザ abc のパスワードの最小長は 16 文字です。

[Sysname] local-user abc class manage
[Sysname-luser-manage-abc] password-control length 16

関連コマンド

- **display local-user (ユーザアクセスと認証/AAA)**
- **display password-control**
- **display user-group (ユーザアクセスと認証/AAA)**
- **password-control length enable**

4.1.16 password-control login idle-time

Syntax

password-control login idle-time *idle-time*

undo password-control login idle-time

デフォルト

ユーザーアカウントのアイドル期間は 90 日間。

View

System view

定義済みユーザロール

network-admin

パラメータ

idle-time:ユーザーアカウントのアイドル時間。値の範囲は 0~365、単位は日です。0 は、ユーザーアカウントのアイドル時間に制限がないことを示します。

説明

password-control login idle-time コマンドを使用して、ユーザーアカウントのアイドル時間を設定します。

undo password-control login idle-time コマンドを使用して、デフォルトの状態を復元します。

ユーザが最後にログインしてから指定されたアイドル時間内にデバイスにログインできなかった場合、ユーザーアカウントは無効になります。

例

#ユーザーアカウントのアイドル時間を 30 日に設定すると、最後にログインに成功してから 30 日以内にデバイスにログインできなければ、ユーザーアカウントは無効になります。

<Sysname> system-view
[Sysname] password-control login idle-time 30

関連コマンド

- **display password-control**

4.1.17 password-control login-attempt

Syntax

password-control login-attempt *login-times* [**exceed** { **lock** | **lock-time** *time* | **unlock** }]

undo password-control login-attempt

デフォルト

グローバルなユーザーログイン試行制限ポリシーは、ユーザーログイン試行の最大回数が 3 回です。ユーザのログイン試行が失敗した場合、そのユーザは 1 分後に再ログインを許可されます。ユーザグループのユーザーログイン試行制限ポリシーグローバルに構成されたユーザーログイン試行制限ポリシー;ローカルユーザのログイン試行回数制限ポリシー所属ユーザグループのログイン試行回数制限ポリシー。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

login-times:ユーザのログイン試行の最大回数。2~10 の値をとります。

exceed:ログイン試行の失敗回数が最大値を超えたユーザの処理。

lock:ログインに失敗した IP アドレスを使用してユーザがログインできないようにします。

lock-time time:ログインに失敗した IP アドレスからのログインを禁止し、時間が経過した後に再ログインを許可することを示します。ここで、 time はそのユーザが禁止されている時間であり、 1~360 の範囲の値をとり、単位は分である。

unlock:ユーザが既存の IP アドレスを使用してログインし続けることを禁止しないことを示します。

説明

password-control login-attempt コマンドを使用して、ユーザがログインできる最大試行回数と、ログイン試行が失敗した後の処理を設定します。

undo password-control login-attempt コマンドを使用して、デフォルトの状態を復元します。

System view の下の構成はグローバルで、すべてのユーザグループに対して有効であり、User group view の下の構成はユーザグループ内のすべてのローカルユーザに対して有効であり、ローカル User view の下の構成は現在のローカルユーザに対してのみ有効です。

構成が有効になる優先度は、「ローカルユーザ」、「ユーザグループ」、「グローバル」の順になります。すなわち、システムはローカル User view での配置を優先し、ローカル User view で配置されていなければ User group view での配置を採用し、User group view でも配置されていなければグローバルビューでの配置を採用する。

FTP ユーザまたは VTY 経由でデバイスにアクセスするユーザのログイン認証が失敗すると、ユーザ名と IP アドレスがパスワード管理のブラックリストに追加されます。ログインに失敗した回数が指定された回数を超えると、その後のログイン動作は、ここで設定された処理に基づいて制限され、ユーザは適切な条件を満たした場合にのみ再ログインできます。

- ログインが完全に禁止されているユーザは、管理者が **reset password-control blacklist** コマンドを使用してパスワード管理のブラックリストからそのユーザを削除するまで、再ログインできません。
- 一定期間ログインが禁止されているユーザは、設定された禁止時間が経過するか、管理者が **reset password-control blacklist** コマンドを使用してパスワード管理のブラックリストから削除するまで、再ログインできません。
- ログインが禁止されていないユーザは、ログインが成功するとすぐにブラックリストから削除されます。

このコマンドが有効になると、パスワード管理ブラックリストに登録されている現在のユーザのロック状態と、その後のユーザのログインに直ちに影響します。

例

#管理者は、ユーザのログイン試行回数を 4 回に設定し、既存の IP アドレスからのログインを永久に禁止します。

```
<Sysname> system-view
[Sysname] password-control login-attempt 4 exceed lock
```

その後、4 回連続して認証を試行して失敗したユーザがいる場合、管理者は、コマンドを使用して、パスワード管理ブラックリストに追加されたユーザのロック状態が以前の unlock から lock に切り替わり、そのユーザが既存の IP アドレスから正常にログインできなくなったことを確認できます。

```
[Sysname] display password-control blacklist
```

Blacklist items matched: 1.

Username	IP address	Login failures	Lock flag
test	192.168.44.1	4	lock

#管理者は、ユーザのログイン試行回数を 2 回に設定し、3 分後に再ログインできるように制限します。

<Sysname> system-view
[Sysname] password-control login-attempt 2 exceed lock-time 3

その後、ユーザが連続して認証を試行した失敗の累積回数が 2 回に達した場合、管理者はコマンドを使用して、パスワード管理ブラックリストに追加されたユーザのロック状態が以前の unlock から lock に変更されたことを確認できます。

[Sysname] display password-control blacklist
Blacklist items matched: 1.

Username	IP address	Login failures	Lock flag
test	192.168.44.1	2	lock

ユーザが既存の IP アドレスからのログインを禁止されてから 3 分が経過すると、パスワード管理ブラックリストから削除され、再度ログインできるようになります。

関連コマンド

- **display local-user (ユーザアクセスと認証/AAA)**
- **display password-control**
- **display password-control blacklist**
- **display user-group (ユーザアクセスと認証/AAA)**
- **reset password-control blacklist**

4.1.18 password-control super aging

Syntax

password-control super aging *aging-time*

undo password-control super aging

デフォルト

パスワードのエージングタイムは 90 日です。

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time:super パスワードのエージングタイム。1~365 の範囲で、単位は日です。

説明

password-control super aging コマンドを使用して、super パスワードのエージングタイムを設定します。

undo password-control super aging コマンドを使用して、デフォルトの状態を復元します。

例

#super パスワードのエージングタイムを 10 日に設定します。

<Sysname> system-view
[Sysname] password-control super aging 10

関連コマンド

- **display password-control**
- **password-control aging**

4.1.19 password-control super composition

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

デフォルト

super パスワードの要素の最小組み合わせタイプと各要素の数は、デバイスのモデルに依存します。デバイスの実際の状態に基づいてください。

View

System view

定義済みユーザロール

network-admin

パラメータ

type-number type-number:super パスワードの最小組み合わせタイプ。ここで、type-number は複合タイプを表し、値の範囲は 1~4 です。

type-length type-length:super パスワードの各タイプの最小文字数。ここで、type-length は文字の数で、範囲は 1~63 です。

説明

password-control super composition コマンドは、super パスワードの組み合わせポリシーを設定するために使用します。

undo password-control super composition コマンドを使用して、デフォルトの状態を復元します。

パスワード要素の最小の組み合わせタイプの数と各要素の最小数の積は、パスワードに許可されている最大長を超えることはできません。

例

#設定 super パスワードの最小組み合わせタイプは 4 つで、各タイプの最小文字数は 5 文字です。

<Sysname> system-view
[Sysname] password-control super composition type-number 4 type-length 5

関連コマンド

- **display password-control**
- **password-control composition**

4.1.20 password-control super length

Syntax

password-control super length *length*

undo password-control super length

デフォルト

super パスワードの最小長はデバイスのモデルに依存します。デバイスの実際の状態に基づいてください。

View

System view

定義済みユーザロール

network-admin

パラメータ

length:super パスワードの最小文字数。範囲は 4~63 です。

説明

password-control super length コマンドを使用して、super パスワードの最小長を設定します。

undo password-control super length コマンドを使用して、デフォルトの状態を復元します。

例

#super パスワードの最小長を 16 文字に設定します。

<Sysname> system-view
[Sysname] password-control super length 16

関連コマンド

- **display password-control**
- **password-control length**

4.1.21 password-control update-interval

Syntax

password-control update-interval *interval*

undo password-control update-interval

デフォルト

パスワード更新の最小間隔は 24 時間です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:パスワードの更新間隔の最小値。0~168 の範囲で、時間単位で指定します。0 は、パスワードの更新間隔に制限がないことを示します。

説明

password-control update-interval コマンドを使用して、パスワード更新の最小間隔を設定します。

undo password-control update-interval コマンドを使用して、デフォルトの状態を復元します。

この機能は、ユーザがデバイスに初めてログインしたときにパスワードの変更を要求される場合など、パスワードの更新には適用されません。パスワードが古くなると、ユーザはパスワードを変更する必要があります。

例

#パスワード更新の最小間隔を 36 時間に設定します。

<Sysname> system-view
[Sysname] password-control update-interval 36

関連コマンド

- **display password-control**

4.1.22 reset password-control blacklist

Syntax

reset password-control blacklist [**user-name** *user-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*:パスワード管理ブラックリストで指定されたユーザをクリアします。ここで、user-name はユーザ名を表します。は 1~80 文字の文字列で、大文字と小文字が区別されます。

説明

reset password-control blacklist コマンドは、パスワード管理ブラックリストからユーザをクリアするために使用します。

ログイン認証時のパスワード試行の失敗回数が最大値を超えたために既存の IP アドレスからのログインが禁止されているユーザは、管理者がこのコマンドを使用してブラックリストから削除し、再ログインできるようにすることができます。

例

#パスワード管理ブラックリストからユーザ test をクリアします。

<Sysname> reset password-control blacklist user-name test
Are you sure to delete the specified user in blacklist?[Y/N]:

関連コマンド

- **display password-control blacklist**

4.1.23 reset password-control history-record

Syntax

reset password-control history-record [**super** [**role** *role-name*] | **user-name** *user-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

super:super パスワードの履歴を削除します。

role role-name:指定されたユーザロールのユーザパスワード履歴を削除します。ここで、role-name はユーザロールを表し、1~63 文字の文字列で、大文字と小文字が区別されます。パラメータを指定しない場合、super パスワードの履歴はすべて削除されます。

user-name user-name:指定したユーザ名のパスワード履歴を削除します。ここで、user-name はユーザ名を表します。は 1~80 文字の文字列で、大文字と小文字が区別されます。

説明

reset password-control history-record コマンドを使用して、ユーザのパスワード履歴をクリアします。

パラメータを指定しない場合、すべてのローカルユーザのパスワード履歴が削除されます。

例

#すべてのローカルユーザのパスワード履歴をクリアします。ユーザが Y と入力すると、すべてのローカルユーザのパスワード履歴が削除されます。

<Sysname> reset password-control history-record

```
Are you sure to delete all local users'history records?[Y/N]:y
All historical passwords have been cleared.
```

関連コマンド

- **password-control history**

目次

このセクションのページは **15-x-x** です。

5 章 公開鍵 5-1
5.1 公開鍵設定コマンド 5-1
5.1.1 display public-key local public 5-1
5.1.2 display public-key peer 5-7
5.1.3 peer-public-key end 5-9
5.1.4 public-key local create 5-10
5.1.5 public-key local destroy 5-14
5.1.6 public-key local export dsa 5-16
5.1.7 public-key local export rsa 5-19
5.1.8 public-key peer 5-21
5.1.9 public-key peer import sshkey 5-23

5章 公開鍵

5.1 公開鍵設定コマンド

5.1.1 display public-key local public

Syntax

display public-key local { **dsa** | **ecdsa** | **rsa** | **sm2** } **public** [**name** *key-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dsa:ローカル DSA 鍵ペアの公開鍵情報を表示します。

ecdsa:ローカル ECDSA キーペアの公開キー情報を表示します。

rsa:ローカル RSA 鍵ペアの公開鍵情報を表示します。

sm 2:ローカル SM 2 キーペアの公開キー情報を表示します。

name key-name:指定されたローカル非対称鍵ペアの公開鍵情報を表示します。key-name は、ローカル非対称キーペアの名前です。1~64 文字の文字列で、大文字と小文字は区別されません。文字列には、文字、数字、および 「-」 を含めることができます。このパラメータを指定しない場合、指定したタイプのすべてのローカル非対称鍵ペアの公開鍵情報が表示されます。

説明

display public-key local public コマンドを使用して、ローカル非対称鍵ペアの公開鍵情報を表示します。

ローカルのホスト公開鍵をリモート・デバイスに手動構成で保存する場合は、ローカルデバイスでこのコマンドを実行してホスト公開鍵情報を表示し、その情報を記録しておく必要があります。

デフォルト名のキーペアの場合、name key-name パラメータを指定して表示することはできません。指定したタイプのローカル非対称キーペアをすべて表示すると、デフォルト名のキーペアが表示されます。

例

#すべてのローカル RSA キーペアの公開キー情報を表示します。

<Sysname> display public-key local rsa public

```
==========================================
Key name:hostkey (default)
Key type:RSA
Key length:1024
Time when key pair created:15:40:48 2011/05/12
Key code:
30819 F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
667269 BB 8226 E 26331 E 30 F 41 A 8 FF 922 C E84332610632B49F75DABF6D871B80CE
7338208097
C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
2 DA4C04EF5AE0835090203010001
==========================================
Key name:serverkey (default)
Key type:RSA
Key length:768
Time when key pair created:15:40:48 2011/05/12
Key code:
307 C300D06092A864886F70D0101010500036B003068026100CAB4CACCA16442AD5F453442
762 F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
9 D 85 C 13413996 ECD 093 B 0203010001
==========================================
Key name:rsa 1
Key type:RSA
Key length:1024
Time when key pair created:15:42:26 2011/05/12
Key code:
30819 F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
426 E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
1 A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
9 A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
92 D8C6D940890BF4290203010001
```

#すべてのローカル DSA キーペアの公開キー情報を表示します。

<Sysname> display public-key local dsa public

```
==========================================
Key name:dsakey (default)
```

```
Key type:DSA
Key length:1024
Time when key pair created:15:41:37 2011/05/12
Key code:
308201 B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
96 E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
7811 C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4 EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
35 D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
91 C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
585 DA7F42519718CC9B09EEF038184000218041912CE34D12BCD2157E7AB1C2F03B3EF395
100 F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
52 DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
887 E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
=============================================
Key name:dsa 1
Key type:DSA
Key length:1024
Time when key pair created:15:35:42 2011/05/12
Key code:
308201 B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
96 E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
7811 C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4 EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
35 D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
91 C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
585 DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
3642 B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
0 FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
15 F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

#すべてのローカル ECDSA キーペアの公開キー情報を表示します。

<Sysname> display public-key local ecdsa public

```
=============================================
Key name:ecdsakey (default)
Key type:ECDSA
Key length:192
Time when key pair created:15:42:04 2011/05/12
Key code:
```

```
3049301306072 A8648CE3D020106082A8648CE3D03010103320004C10CF7CE42193F7FC2AF
68 F5DC877835A43009DB6135558A7FB8316C361B0690B4FD84A14C0779C76DD6145BF9362B
1D
=============================================
Key name:ecdsa1
Key type:ECDSA
Key length:192
Time when key pair created:15:43:33 2011/05/12
Key code:
3049301306072 A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
4D
```

#すべてのローカル SM 2 キーペアの公開キー情報を表示します。

<Sysname> display public-key local sm2 public

```
=============================================
Key name:sm2key (default)
Key type:SM 2
Key length:256
Time when key pair created:15:42:04 2016/08/15
Key code:
3059301306072 A8648CE3D020106082A811CCF5501822D03420004DC5D3CCDD4F5E7AC9803
D7F55ADC0668C067859482999C390B1648BE91FB567150A6C909706BB04AFE8709D5EC884C
BD4EE36F38E8AD7DBCFB52286BF22CB146
=============================================
Key name:sm 21
Key type:SM 2
Key length:256
Time when key pair created:15:43:33 2016/08/15
Key code:
3059301306072 A8648CE3D020106082A811CCF5501822D034200047A8EF255A75A90FA9239
1 B2BDD58B6F19E7D0158200E80297E434109A68A66160A20B5267ECB1706CA50A7ED04A89A
007 AFEFF 8335441347 EB2EB69CFB4CD459
```

#rsa 1 という名前のローカル RSA キーペアの公開キー情報を表示します。

<Sysname> display public-key local rsa public name rsa1

```
=============================================
Key name:rsa 1
Key type:RSA
Key length:1024
Time when key pair created:15:42:26 2011/05/12
Key code:
```

```
30819 F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
426 E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
1 A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
9 A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
92 D8C6D940890BF4290203010001
```

#dsa 1 という名前のローカル DSA キーペアの公開キー情報を表示します。

<Sysname> display public-key local dsa public name dsa1

```
=========================================
Key name:dsa 1
Key type:DSA
Key length:1024
Time when key pair created:15:35:42 2011/05/12
Key code:
308201 B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
96 E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
7811 C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4 EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
35 D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
91 C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
585 DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
3642 B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
0 FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
15 F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

#ecdsa1 という名前のローカル ECDSA キーペアの公開キー情報を表示します。

<Sysname> display public-key local ecdsa public name ecdsa1

```
=========================================
Key name:ecdsa1
Key type:ECDSA
Key length:192
Time when key pair created:15:43:33 2011/05/12
Key code:
3049301306072 A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
4D
```

#sm 21 という名前のローカル SM 2 キーペアの公開キー情報を表示します。

<Sysname> display public-key local sm2 public name sm21

```
=========================================
Key name:sm 21
```

```
Key type:SM 2
Key length:256
Time when key pair created:15:43:33 2016/08/15
Key code:
3059301306072 A8648CE3D020106082A811CCF5501822D034200047A8EF255A75A90FA9239
1 B2BDD58B6F19E7D0158200E80297E434109A68A66160A20B5267ECB1706CA50A7ED04A89A
007 AFEFF 8335441347 EB2EB69CFB4CD459
```

#暗号化デバイスによって生成された SM 2 キーペア sm-hardware の公開キー情報を表示します。

<Sysname> display public-key local sm2 public name sm2-hardware

```
==========================================
Key name:sm2-hardware
Key type:SM 2
Key length:256
Storage device serial number:2016091400125014
Time when key pair created:08:52:02 2017/09/06
Key code:
043685 DF 5943674 D 61 D 096 D 3218 C 235728467 ED 4699893777
EB2D4D77D302B44DC87C587A0
7 A9EC72802BCB13EFAF77E0E744FB49FA8C2A23BCDE7BB1E91462697
```

表 5-1 display public-key local public コマンドの表示情報の説明

フィールド	説明
Key name	ローカル非対称キーペアの名前 defaultは、この名前がキーペアのデフォルト名であることを示します。つまり、public-key local createコマンドを実行してキー名を指定しなかった場合に生成されるキーペアの名前です。 • hostkey:RSA ホストキーペアのデフォルト名 • serverkey:RSA サーバキーペアのデフォルト名。サーバキーペアは、キータイプが RSA の場合にのみ存在します。 • dsakey:DSA ホストキーペアのデフォルト名 • ecdsakey:ECDSA ホストキーペアのデフォルト名 • sm2key:SM 2 ホストキーペアのデフォルト名

フィールド	説明
Key type	キーのタイプ。値は次のとおりです。 • RSA:キータイプ RSA • DSA:キータイプ DSA • ECDSA:キータイプ ECDSA • SM 2:キータイプ SM 2
Key length	キーの長さ、単位はビット
Storage device serial number	キーペアの暗号化デバイスシリアル番号を生成します。キーペアがソフトウェアアルゴリズムによって生成された場合、このフィールドは表示されません。
Time when key pair created	ローカル非対称鍵ペアの生成時刻
Key code	ローカル非対称鍵ペアの公開鍵データ

関連コマンド

- **public-key local create**

5.1.2 display public-key peer

Syntax

display public-key peer [**brief** | **name** *publickey-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

brief:ローカルに保存されているすべてのリモートホスト公開キーの簡単な情報を表示します。

name publickey-name:ローカルに保存されている指定されたリモートホスト公開鍵の詳細を表示します。publickey-name はリモートホスト公開鍵の名前で、1~64 文字の文字列で、大文字と小文字が区別されます。

説明

display public-key peer コマンドは、ローカルに保存されているリモートホストの公開鍵情報を表示するために使用されます。

パラメータを指定しない場合は、ローカルに保存されているすべてのリモートホスト公開キーの詳細が表示されます。

リモートホストの公開鍵は、**public-key peer** コマンドまたは **public-key peer import sshkey** コマンドを使用してローカルに構成できます。

例

#ローカルに保存されている idrsa という名前のリモートホスト公開鍵の詳細を表示します。

<Sysname> display public-key peer name idrsa

```
=========================================
Key name:idrsa
Key type:RSA
Key length:1024
Key code:
30819 F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
918 F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
6 D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
42 C 142 D 41 BB 4884 FEB 0203010001
```

表 5-2 display public-key peer name コマンドの表示情報の説明

フィールド	説明
Key name	リモートホストの公開鍵の名前
Key type	RSA、DSA、ECDSAなどのキータイプ
Key length	キーの長さ、単位はビット
Key code	公開鍵データ

#ローカルに保存されているすべてのリモートホスト公開キーの簡単な情報を表示します。

<Sysname> display public-key peer brief

```
TypeModulusName
--------------------------
RSA1024idrsa
DSA102410.1.1.1
```

表 5-3 display public-key peer brief コマンドの表示情報の説明

フィールド	説明
Type	RSA、DSA、ECDSAなどのキータイプ
Modulus	キーモジュールの長さ。単位はビットです。
Name	リモートホストの公開鍵の名前

関連コマンド

- **public-key peer**
- **public-key peer import sshkey**

5.1.3 peer-public-key end

Syntax

peer-public-key end

View

Public key view

定義済みユーザロール

network-admin

説明

peer-public-key end コマンドを使用すると、Public key view から System view に戻り、ユーザーが入力した公開鍵を保存できます。

このコマンドは、リモートホストの公開キーを手動設定でローカルデバイスに保存するために使用します。手動設定方法は次のとおりです。

(1) **public-key peer** コマンドを実行して、Public key view に移動します。

(2) リモートホストの公開鍵を Public key view に手動で入力します。

(3) **peer-public-key end** コマンドを実行して Public key view を終了し、入力した公開鍵を保存します。

入力する公開鍵データは、一定のフォーマットを満たす必要がある。公開鍵を保存する前に、デバイスは公開鍵の正当性を検査します。

- ユーザーが設定した公開鍵文字列がフォーマットの要件を満たしていない場合は、プロンプトが表示され、ユーザーが設定した公開鍵は破棄されます。この設定は失敗します。
- 入力された公開鍵データが **display public-key local public** コマンドで表示された公開鍵であるなど、ユーザーが構成した公開鍵文字列が正当な場合は、その公開鍵を保存します。

例

#Public key view を終了し、ユーザーが入力した公開鍵を保存します。

<Sysname> system-view

[Sysname] public-key peer key1

```
Enter public key view.Return to system view with "peer-public-key end" command.
```

[Sysname-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D0030818902818100C0EC8014F82515F6335A0A

[Sysname-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C29481B77E719D1643135877E13B1C531B4

[Sysname-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854E2371D5B952ADF6B80EB5F52698FCF3D6

[Sysname-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276FFD4AF2050BD4A9B1DDE675AC30CB020301

[Sysname-pkey-public-key-key1]0001

[Sysname-pkey-public-key-key1] peer-public-key end

[Sysname]

関連コマンド

- **display public-key local public**
- **display public-key peer**
- **public-key peer**

5.1.4 public-key local create

Syntax

public-key local create { **dsa** | **ecdsa** [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**] | **rsa** } [**name** *key-name*]

public-key local create sm2 [**name** *key-name*] [**on** *device-name*]

デフォルト

ローカル非対称キーペアは存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

dsa:ローカルキーペアタイプは DSA です。

ecdsa:ローカルキーペアのタイプは ECDSA です。

- *secp192r1*:ローカル ECDSA 鍵ペアを、鍵長 192 ビットの secp192r1 という楕円曲線を用いて生成する。
- *secp256r1*:ローカル ECDSA 鍵ペアを、鍵長 256 ビットの secp256r1 という楕円曲線を用いて生成する。
- *secp384r1*:ローカル ECDSA 鍵ペアを secp384r1 という名前の楕円曲線を用いて生成し、鍵長は 384 ビットである。
- *secp521r1*:ローカル ECDSA 鍵ペアを、鍵長 521 ビットの secp521r1 という楕円曲線を用いて生成する。

上記の鍵ペアアルゴリズムパラメータのいずれも指定しない場合、ローカル ECDSA 鍵ペアは、鍵長 192 ビットの secp192r1 という名前の楕円曲線を用いて生成される。

rsa:ローカルキーペアタイプは RSA です。

sm 2:ローカルキーペアタイプは SM 2 です。

name key-name:指定した名前のローカル非対称キーペアを生成します。key-name はローカル非対称キーペアの名前で、1~64 文字の文字列です。大文字と小文字は区別されず、文字、数字、および 「-」 のみを使用できます。このパラメータを指定しない場合、生成される RSA ホストキーペアのデフォルト名は hostkey、RSA サーバキーペアのデフォルト名は serverkey、DSA キーペアのデフォルト名は dsakey、ECDSA キーペアのデフォルト名は ecdsakey、SM 2 キーペアのデフォルト名は sm2key です。

on device-name:SM 2 キーペアを生成する暗号化デバイスを指定します。device-name は暗号化デバイス名で、大文字と小文字を区別する 1~31 文字の文字列を指定します。本パラメータを指定しない場合、ソフトウェアアルゴリズムにより秘密鍵ペアが生成されることを示す。ユーザーは、ヘルプ情報から現在のデバイスで使用可能な暗号化されたデバイス名を取得できます。

説明

public-key local create コマンドを使用して、非対称鍵ペアを生成します。

RSA キーと DSA キーのペアを作成すると、キーモジュールの長さの入力を求めるプロンプトが表示されます。鍵モジュールが長いほどセキュリティは向上するが、鍵の生成に時間がかかる。ECDSA キーペアを作成するときは、キーの長さが異なる楕円曲線を使用できます。キーが長いほどセキュリティは向上しますが、キーの生成に時間がかかります。SM 2 キーペアを作成するときは、固定キー長の楕円曲線を使用します。キーモジュールの長さに関する設定上の制限と考慮事項については、表 5-4 を参照してください。

キーペアを生成するときにキーペア名を指定しないと、キーペアにデフォルトの名前が付けられ、デフォルトとしてマークされます(default)。

ユーザーはデフォルトのキーペア名を使用して別のキーペアを作成できますが、そのキーペアはデフォルトとしてマークされません(default)。

デフォルト以外の名前キーペアのキータイプと名前は同じにすることはできません。同じにしない場合は、元のキーペアを上書きするかどうかをユーザーが確認する必要があります。同じ名前を持つ異なるタイプのキーペア。

このコマンドを実行すると、生成されたキーペアはデバイスに保存され、デバイスを再起動してもキーは失われません。

表 5-4　異なるタイプのキーペアの比較

キーペアタイプ	生成された鍵ペア	鍵モジュール長
RSA	• キーペア名を指定しない場合、サーバキーペアとホストキーペアの2つのキーペアが同時に生成されます。 • キーペア名を指定すると、1つのホストキーペアのみが生成されます。 🕮 メモ　： 現在、RSAサーバキーペアが適用されているのはSSH1.5だけです。	長さの範囲は512~2048ビットで、デフォルト値は1024ビットです。768ビット以上の鍵モジュールを推奨します。
DSA	ホスト鍵ペアを1つだけ生成	長さの範囲は512~2048ビットで、デフォルト値は1024ビットです。768ビット以上の鍵モジュールを推奨します。
ECDSA	ホスト鍵ペアを1つだけ生成	長さは192、256、384、または521ビットの値をとります。

例

#デフォルト名のローカル RSA 非対称キーペアを生成します。

<Sysname> system-view
[Sysname] public-key local create rsa

```
The range of public key modulus is (5 12~2048).
If the key modulus is greater than 512，it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default =1024]:
Generating Keys ...
...++++++
.++++++
..++++++++
....++++++++
Create the key pair successfully.
```

#デフォルト名のローカル DSA 非対称キーペアを生成します。

<Sysname> system-view
[Sysname] public-key local create dsa

```
The range of public key modulus is (5 12~2048).
If the key modulus is greater than 512、it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default =1024]:
Generating Keys ...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+..........+.............+.............+...+.....+..............+..+
...+.................+..........+...+....+.......+.....+............+.......+.
.........................+........+..........+..............+.....+...+.......
..............+.........+..........+...........+........+....+...............
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

#デフォルト名のローカル ECDSA 非対称キーペアを生成します。

```
<Sysname> system-view
[Sysname] public-key local create ecdsa
Generating Keys ...
Create the key pair successfully.
```

#デフォルト名のローカル SM 2 非対称キーペアを生成します。

```
<Sysname> system-view
[Sysname] public-key local create sm2
Generating Keys ...
Create the key pair successfully.
```

#rsa 1 という名前のローカル RSA 非対称キーペアを生成します。

```
<Sysname> system-view
[Sysname] public-key local create rsa name rsa1
The range of public key modulus is (5 12~2048).
If the key modulus is greater than 512、it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default =1024]:
Generating Keys ...
...++++++
.............................++++++
Create the key pair successfully.
```

#dsa 1 という名前のローカル DSA 非対称キーペアを生成します。

```
<Sysname> system-view
[Sysname] public-key local create dsa name dsa1
The range of public key modulus is (5 12~2048).
If the key modulus is greater than 512、it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default =1024]:
```

```
Generating Keys ...
.++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+..........+.............+.............+...+.....+..............+..+
...+................+..........+...+....+.......+.....+............+........
.........................+........+..........+..............+.....+...+.......
..............+.........+..........+...........+........+....+...............
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

#ecdsa1 という名前のローカル ECDSA 非対称キーペアを生成します。

<Sysname> system-view
[Sysname] public-key local create ecdsa name ecdsa1

```
Generating Keys ...
Create the key pair successfully.
```

#sm 2 という名前のローカル SM 2 非対称キーペアを生成します。

<Sysname> system-view
[Sysname] public-key local create sm2 name sm2

```
Generating Keys ...
Create the key pair successfully.
```

関連コマンド

- **display public-key local public**
- **public-key local destroy**

5.1.5 public-key local destroy

Syntax

public-key local destroy { **dsa** | **ecdsa** | **rsa**| **sm2** } [**name** *key-name*]

View

System view

定義済みユーザロール

network-admin

パラメータ

dsa:ローカルキーペアタイプは DSA です。

ecdsa:ローカルキーペアのタイプは ECDSA です。

rsa*:*ローカルキーペアタイプは RSA です。

sm 2:ローカルキーペアタイプは SM 2 です。

name key-name:指定した名前のローカル非対称キーペアを破棄します。key-name は、ローカル非対称キーペア名で、大文字と小文字を区別しない 1~64 文字の文字列です。文字列には、文字、数字、 「-」 を含めることができます。このパラメータを指定しない場合、指定したタイプのデフォルト名のローカル非対称キーペアを破棄します。

説明

public-key local destroy コマンドを使用して、ローカル非対称キーペアを破棄します。

次のような場合は、古い非対称鍵ペアを破棄し、新しい鍵ペアを生成することをお勧めします。

- ローカルデバイスのプライベートキーが漏洩しました。この場合、不正なユーザーがローカルデバイスになりすましてネットワークにアクセスする可能性があります。
- キーペアを保存するストレージデバイスで障害が発生したため、デバイスに公開キーに対応する秘密キーがなく、古い非対称キーペアを使用して暗号化とデジタル署名を行うことができなくなりました。
- キーペアの使用時間が長くなると、キーが漏洩または解読される可能性があります。
- ローカル証明書が有効期限に達したら、対応するローカルキーペアを削除する必要があります。

例

#デフォルト名のローカル RSA 非対称キーペアを破棄します。

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Confirm to destroy the key pair?[Y/N]:y
```

#デフォルト名のローカル DSA 非対称キーペアを破棄します。

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Confirm to destroy the key pair?[Y/N]:y
```

#デフォルト名のローカル ECDSA 非対称キーペアを破棄します。

```
<Sysname> system-view
[Sysname] public-key local destroy ecdsa
Confirm to destroy the key pair?[Y/N]:y
```

#デフォルト名のローカル SM 2 非対称キーペアを破棄します。

```
<Sysname> system-view
[Sysname] public-key local destroy sm2
Confirm to destroy the key pair?[Y/N]:y
```

#rsa 1 という名前のローカル RSA 非対称キーペアを破棄します。

```
<Sysname> system-view
[Sysname] public-key local destroy rsa name rsa1
Confirm to destroy the key pair?[Y/N]:y
```

#dsa 1 という名前のローカル DSA 非対称キーペアを破棄します。

<Sysname> system-view
[Sysname] public-key local destroy dsa name dsa1
Confirm to destroy the key pair?[Y/N]:y

#ecdsa1 という名前のローカル ECDSA 非対称キーペアを破棄します。

<Sysname> system-view
[Sysname] public-key local destroy ecdsa name ecdsa1
Confirm to destroy the key pair?[Y/N]:y

#sm 2 という名前のローカル SM 2 非対称キーペアを破棄します。

<Sysname> system-view
[Sysname] public-key local destroy sm2 name sm2
Confirm to destroy the key pair?[Y/N]:y

関連コマンド

- **public-key local create**

5.1.6 public-key local export dsa

Syntax

public-key local export dsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

View

System view

定義済みユーザロール

network-admin

パラメータ

name key-name:指定したローカル DSA キーペアのホスト公開キーを表示またはエクスポートします。key-name はローカルキーペアの名前で、大文字と小文字を区別しない 1~64 文字の文字列です。文字列には、文字、数字、および 「-」 を含めることができます。このパラメータを指定しない場合は、デフォルト名のローカル DSA キーペアのホスト公開キーを表示またはエクスポートします。

openssh:ホストの公開キーの形式は OpenSSH です。

ssh 2:ホストの公開キーの形式は SSH2.0 です。

filename:エクスポートされた公開鍵が格納されているファイルの名前を指定します。大文字と小文字は区別されず、「hostkey」、「serverkey」、「dsakey」、「ecdsakey」の値は使用できません。また、すべて 「.」 は使用できません。また、最初の文字は 「/」 は使用できず、文字列「.」と「../」は使用できません。ファイル名は 1~128 文字の文字列です。ファイル名の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*10 章 ファイルシステム管理*”を参照してくだ

さい。このパラメータを指定しない場合は、指定した形式でローカル DSA ホストの公開鍵が表示されます。

説明

public-key local export dsa コマンドは、指定された形式でローカル DSA ホストの公開鍵を表示したり、指定されたファイルにエクスポートしたりするために使用します。

ローカルホストの公開鍵をリモート・デバイスに保存するには、公開鍵ファイルからインポートします。

(1) 次のいずれかの方法で、エクスポートされた公開キーをファイルに保存します。

- ローカルデバイスで **public-key local export** コマンドを実行すると、ローカルホストの公開鍵(コマンドの実行時に filename パラメータを指定しない)が指定した形式で表示されます。表示されたホストの公開鍵は、貼り付けコピーによってファイルに保存されます。
- ローカルデバイスで **public-key local export** コマンドを実行して、指定した形式でローカルホストの公開鍵を指定したファイル(コマンドの実行時に filename パラメータを指定する)にエクスポートします。ホストの公開鍵は、作業パスの pkey ディレクトリおよび pkey のサブディレクトリにエクスポートできないことに注意してください。

(2) 取得した証明書ファイルを FTP バイナリモードまたは TFTP 経由でリモートホストにアップロードします。FTP および TFTP の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*8 章 FTP*”および”*9 章 TFTP*”を参照してください。

(3) リモートホストで、**public-key peer import sshkey** コマンドを実行してホストの公開鍵をローカルに保存します。

SSH 2.0 と OpenSSH は異なる公開鍵形式です。ホスト公開鍵をインポートするデバイスでサポートされている正しい形式を選択します。

例

#デフォルト名のローカル DSA キーペアのホスト公開キーを OpenSSH 形式でエクスポートします。エクスポートされた公開キーを格納するファイル名は key.pub です。

<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub

#デフォルト名のローカル DSA キーペアのホスト公開キーを SSH2.0 形式で表示します。

<Sysname> system-view
[Sysname] public-key local export dsa ssh2

```
---- BEGIN SSH 2 PUBLIC KEY ----
Comment:"dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
```

```
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBt
YcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3sTwmIflQeweU
wLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=
---- END SSH 2 PUBLIC KEY ----
```

#デフォルト名のローカル DSA キーペアのホスト公開キーを OpenSSH 形式で表示します。

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBt
YcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3sTwmIflQeweU
wLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=dsa-key
```

#dsa 1 という名前のローカル DSA キーペアのホスト公開キーを OpenSSH 形式でエクスポートします。ファイル名は dsa1.pub です。

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 openssh dsa1.pub
```

#名前が dsa 1 のローカル DSA キーペアのホスト公開キーを SSH2.0 形式で表示します。

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 ssh2
---- BEGIN SSH 2 PUBLIC KEY ----
Comment:"dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3
ES9XFD7gIK70pb+tB7dA+8
scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+q
BAD4WcpSX0OrZEF4+dq
---- END SSH 2 PUBLIC KEY ----
```

#名前が dsa 1 のローカル DSA キーペアのホスト公開キーを OpenSSH 形式で表示します。

```
<Sysname> system-view
[Sysname] public-key local export dsa name dsa1 openssh
```

```
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3
ES9XFD7gIK70pb+tB7dA+8
scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7CrcV+ft7UUvBF0FV3W4HOx/LOidJ5sX+q
BAD4WcpSX0OrZEF4+dq dsa-key
```

関連コマンド

- **public-key local create**
- **public-key peer import sshkey**

5.1.7 public-key local export rsa

Syntax

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*]

View

System view

定義済みユーザロール

network-admin

パラメータ

name key-name:指定したローカル RSA キーペアのホスト公開キーを表示またはエクスポートします。key-name はローカルキーペアの名前で、大文字と小文字を区別しない 1~64 文字の文字列です。文字列には、文字、数字、および 「-」 を含めることができます。このパラメータを指定しない場合は、デフォルト名のローカル RSA キーペアのホスト公開キーを表示またはエクスポートします。

openssh:ホストの公開キーの形式は OpenSSH です。

ssh 1:ホストの公開キーの形式は SSH1.5 です。

ssh 2:ホストの公開キーの形式は SSH2.0 です。

filename:エクスポートされた公開鍵が格納されているファイルの名前を指定します。大文字と小文字は区別されず、「hostkey」、「serverkey」、「dsakey」、「ecdsakey」の値は使用できません。また、すべて 「.」 は使用できません。また、最初の文字は 「/」 は使用できず、文字列「.」と「../」は使用できません。ファイル名は 1~128 文字の文字列です。ファイル名の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*10 章 ファイルシステム管理*”を参照してください。

このパラメータを指定しない場合は、指定した形式でローカル RSA ホストの公開キーが表示されます。

説明

public-key local export rsa コマンドを使用すると、ローカル RSA ホストの公開鍵を指定した形式で表示したり、指定したファイルにエクスポートしたりできます。

ローカルホストの公開鍵をリモート・デバイスに保存するには、公開鍵ファイルからインポートします。

(1) 次のいずれかの方法で、エクスポートされた公開キーをファイルに保存します。

- ローカルデバイスで **public-key local export** コマンドを実行すると、ローカルホストの公開鍵(コマンドの実行時に filename パラメータを指定しない)が指定した形式で表示されます。表示されたホストの公開鍵は、貼り付けコピーによってファイルに保存されます。
- ローカルデバイスで **public-key local expor**t コマンドを実行して、指定した形式でローカルホストの公開鍵を指定したファイル(コマンドの実行時に filename パラメータを指定する)にエクスポートします。ホストの公開鍵は、作業パスの pkey ディレクトリおよび pkey のサブディレクトリにエクスポートできないことに注意してください。

(2) 取得した証明書ファイルを FTP バイナリモードまたは TFTP 経由でリモートホストにアップロードします。FTP および TFTP の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*8 章 FTP*”および”*9 章 TFTP*”を参照してください。

(3) リモートホストで、public-key peer import sshkey コマンドを実行してホストの公開鍵をローカルに保存します。

SSH1.5、SSH2.0、および OpenSSH は、サーバ側でサポートされているピア公開鍵フォーマットに基づいて、エクスポートされるホスト公開鍵フォーマットを選択する必要がある、3 種類の公開鍵フォーマットです。

例

#デフォルト名のローカル RSA キーペアのホスト公開キーを OpenSSH 形式でエクスポートします。エクスポートされた公開キーは key.pub というファイル名で保存されます。

<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub

#デフォルト名のローカル RSA キーペアのホスト公開キーを SSH2.0 形式で表示します。

<Sysname> system-view
[Sysname] public-key local export rsa ssh2

```
---- BEGIN SSH 2 PUBLIC KEY ----
Comment:"rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGM
rSfddq/bYcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvy
vPJilneKJqhPT0xdv4tlas+mLNloY0dImbwS2kwE71rgg1CQ==
```

```
---- END SSH 2 PUBLIC KEY ----
```

#デフォルト名のローカル RSA キーペアのホスト公開キーを OpenSSH 形式で表示します。

<Sysname> system-view
[Sysname] public-key local export rsa openssh

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGM
rSfddq/bYcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvy
vPJilneKJqhPT0xdv4tlas+mLNloY0dImbwS2kwE71rgg1CQ==rsa-key
```

#rsa 1 という名前のローカル RSA キーペアのホスト公開キーを OpenSSH 形式でエクスポートします。ファイル名は rsa1.pub です。

<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh rsa1.pub

#rsa 1 という名前のローカル RSA キーペアのホスト公開キーを SSH2.0 形式で表示します。

<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 ssh2

```
---- BEGIN SSH 2 PUBLIC KEY ----
Comment:"rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J0
0fBQ8XY+q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05
t8mCLVaupbfCzP8ba8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH 2 PUBLIC KEY ----
```

#rsa 1 という名前のローカル RSA キーペアのホスト公開キーを OpenSSH 形式で表示します。

<Sysname> system-view
[Sysname] public-key local export rsa name rsa1 openssh

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J0
0fBQ8XY+q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05
t8mCLVaupbfCzP8ba8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ==rsa-key
```

関連コマンド

- **public-key local create**
- **public-key peer import sshkey**

5.1.8 public-key peer

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

デフォルト

リモートホストの公開鍵がありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

keyname:リモートホストの公開鍵の名前。1~64 文字の文字列で、大文字と小文字が区別されます。

説明

public-key peer コマンドは、リモートホストの公開鍵の名前を指定し、Public key view を表示します。指定したリモートホストの公開鍵名がすでに存在する場合は、その Public key view に直接移動します。

undo public-key peer コマンドは、指定されたリモートホストの公開鍵を削除します。

Public key view に移動すると、公開鍵データの入力を開始できます。公開鍵データを入力するときは、文字間にスペースを入れるか、Enter キーを押してデータを入力します。公開鍵データを保存すると、スペースと改行文字が削除されます。

手動構成でリモートホストの公開鍵を作成する場合、ユーザーはリモートホストの 16 進形式の公開鍵を事前に取得および記録し、ローカルデバイスで次の操作を実行する必要があります。

(1) Public key view に移動するには、このコマンドを実行します。

(2) Public key view で、リモートホストの公開鍵を手動で入力します。

(3) peer-public-key end コマンドを実行して、入力したリモートホスト公開鍵を保存し、Public key view から System view に戻します。

入力する公開鍵データは、一定のフォーマットを満たす必要がある。**display public-key local public** コマンドで表示される公開鍵は、入力として公開鍵データとすることができる。

例

#リモートホストの公開鍵名を key 1 に指定し、Public key view に移動します。

```
<Sysname> system-view
[Sysname] public-key peer key1
Enter public key view.Return to system view with "peer-public-key end" command.
[Sysname-pkey-public-key-key1]
```

関連コマンド

- **display public-key local public**
- **display public-key peer**
- **peer-public-key end**

5.1.9 public-key peer import sshkey

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

デフォルト

リモートホストの公開鍵がありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

keyname:リモートホストの公開鍵の名前。1~64 文字の文字列で、大文字と小文字が区別されます。

filename:公開鍵データをインポートするファイル名を指定します。大文字と小文字は区別されません。「hostkey」、「serverkey」、「dsakey」、「ecdsakey」の値は使用できません。また、すべて 「.」 は使用できません。また、最初の文字は 「/」 は使用できません。文字列「.」と「../」は使用できません。ファイル名は 1~128 文字の文字列です。ファイル名の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*10 章 ファイルシステム管理*”を参照してください。

説明

public-key peer import sshkey コマンドは、公開鍵ファイルからリモートホストにインポートする公開鍵を設定します。

undo public-key peer コマンドは、指定されたリモートホストの公開鍵を削除します。

このコマンドを実行すると、指定した公開キーファイル内の公開キーが PKCS 標準のエンコード形式に変換され、リモートホストの公開キーがローカルデバイスに保存されます。

リモートホストの公開鍵を公開鍵ファイルからインポートする前に、リモートホストが公開鍵ファイルに保存し、ローカルデバイスにアップロードする必要があります。たとえば、リモートホストで **public-key local export** コマンドを実行すると、公開鍵が公開鍵

ファイルにエクスポートされ、FTP または TFTP を介してローカルデバイスにバイナリで保存されます。

現在、デバイスでサポートされている公開キーの形式は、SSH1.5、SSH2.0、および OpenSSH です。

例

#設定リモートホストの公開鍵を公開鍵ファイル key.pub からインポートします。公開鍵名は key 2 です。

<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub

関連コマンド

- **display public-key peer**
- **public-key local export dsa**
- **public-key local export ecdsa**
- **public-key local export rsa**

目次

このセクションのページは **15-x-x** です。

6 章 SSH 6-1
6.1 SSH サーバ設定コマンド 6-1
6.1.1 display ssh server 6-1
6.1.2 display ssh user-information 6-3
6.1.3 free ssh 6-4
6.1.4 sftp server enable 6-5
6.1.5 sftp server idle-timeout 6-6
6.1.6 ssh server acl 6-7
6.1.7 ssh server acl-deny-log enable 6-8
6.1.8 ssh server authentication-retries 6-9
6.1.9 ssh server authentication-timeout 6-10
6.1.10 ssh server compatible-ssh1x enable 6-11
6.1.11 ssh server dscp 6-11
6.1.12 ssh server enable 6-12
6.1.13 ssh server port 6-13
6.1.14 ssh server rekey-interval 6-14
6.1.15 ssh user 6-15
6.2 SSH クライアント構成コマンド 6-18
6.2.1 bye 6-18
6.2.2 cd 6-18
6.2.3 cdup 6-19
6.2.4 delete 6-20
6.2.5 dir 6-20
6.2.6 display sftp client source 6-21
6.2.7 display ssh client source 6-22
6.2.8 exit 6-23
6.2.9 get 6-23
6.2.10 help 6-24
6.2.11 ls 6-25
6.2.12 mkdir 6-26
6.2.13 put 6-26
6.2.14 pwd 6-27
6.2.15 quit 6-28
6.2.16 remove 6-28
6.2.17 rename 6-29
6.2.18 rmdir 6-29

6.2.19 sftp 6-30
6.2.20 sftp client source 6-33
6.2.21 ssh client source 6-34
6.2.22 ssh 2 6-35
6.3 SSH 2 プロトコル構成コマンド 6-38
6.3.1 display ssh2 algorithm 6-38
6.3.2 ssh2 algorithm cipher 6-40
6.3.3 ssh2 algorithm key-exchange 6-41
6.3.4 ssh2 algorithm mac 6-42
6.3.5 ssh2 algorithm public-key 6-43

6章 SSH

6.1 SSHサーバ設定コマンド

6.1.1 display ssh server

Syntax

display ssh server { **session** | **status** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

session:SSH サーバのセッション情報を表示します。

status:SSH サーバのステータス情報を表示します。

説明

display ssh server コマンドを使用して、SSH サーバ側にサーバのステータス情報またはセッション情報を表示します。

例

#サーバのステータス情報を SSH サーバ側に表示します。

<Sysname> display ssh server status
Stelnet server:Disable
SSH version :2.0
SSH authentication-timeout :60 second (s)
SSH server key generating interval :0 hour (s)
SSH authentication retries :3 time (s)
SFTP server:Disable
SFTP server Idle-Timeout:10 minute (s)
NETCONF server:Disable
SCP server:Disable
SSH Server PKI domain name:aaa

表 6-1 display ssh server status コマンドの表示情報の説明

フィールド	説明
Stelnet server	Stelnetサーバ機能の状態
SSH version	SSHプロトコルバージョン SSHサーバはSSH 1時対応、プロトコルバージョンは1.99;SSHサーバはSSH 1時と互換性がなく、プロトコルバージョンは2.0
SSH authentication-timeout	認証タイムアウト時間
SSH server key generating interval	RSAサーバキーペアの最小更新間隔
SSH authentication retries	SSHユーザ認証試行の最大数
SFTP server	SFTPサーバ機能の状態
SFTP server Idle-Timeout	SFTPユーザ接続のアイドルタイムアウト時間
NETCONF server	(未サポート) NETCONF over SSHサーバ機能の状況
SCP server	SCPサーバ機能の状態
SSH Server PKI domain name	SSHサーバPKIドメイン構成

#サーバのセッション情報を SSH サーバ側に表示します。

<Sysname> display ssh server session

UserPidSessID VerEncryptStateRetriesServUsername

18402.0aes128-cbc Established1Stelnetabc@123

表 6-2 display ssh server session 情報説明表の表示

フィールド	説明
UserPid	ユーザプロセスPID
SessID	セッションID
Ver	SSHサーバのプロトコルバージョン
State	次のセッション・ステータス • Init:初期化ステータス • Ver-exchange:バージョンのネゴシエーション • Keys-exchange:キー交換 • Auth-request:ユーザ認証 • Serv-request:サービスリクエスト • Established:セッションが確立されました • Disconnected:セッションを切断する
Retries	認証に失敗した回数
Serv	SCP、SFTP、Stelnetなどのサービスタイプ

フィールド	説明
Username	クライアントがサーバにログインするときに使用するユーザ名

6.1.2 display ssh user-information

Syntax

display ssh user-information [*username*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

username:SSH ユーザ名。1~80 文字の文字列で、大文字と小文字が区別されます。このパラメータを指定しない場合は、すべての SSH ユーザの情報が表示されます。

説明

display ssh user-information コマンドを使用して、SSH サーバ側に SSH ユーザの情報を表示します。

このコマンドは、**ssh user** コマンドを使用して SSH サーバ側で設定された SSH ユーザ情報を表示する場合にのみ使用します。

例

#すべての SSH ユーザの情報を表示します。

<Sysname> display ssh user-information

Total ssh users:2

Username	Authentication-type	User-public-key-name	Service-type
yemx	password		Stelnet	SFTP
test	publickey	pubkey	SFTP

表 6-3 display ssh user-information 情報説明表の表示

フィールド	説明
Total ssh users	SSHユーザの合計数
Username	ユーザ名
Authentication-type	password、publickey、password-publickey、anyなどの認証タイプ

フィールド	説明
User-public-key-name	ユーザ公開鍵名 認証タイプがpasswordの場合、このフィールドは空白になります。
Service-type	SCP、SFTP、Stelnetなどのサービスタイプ デバイスが同時に複数のSSHサービスタイプを表示する場合は、|で区切ります。

関連コマンド

- **ssh user**

6.1.3 free ssh

Syntax

free ssh { **user-ip** { *ip-address* } [**port** *port-number*] | **user-pid** *pid-number* | **username** *username* }

View

User view

定義済みユーザロール

network-admin

パラメータ

user-ip:確立された SSH 接続を IP アドレスに基づいて強制的に解放します。

ip-address:解放される SSH 接続の送信元 IPv 4 アドレス。

port *port-number*:解放する SSH 接続の送信元ポート。port-number は送信元ポート番号で、範囲は 1~65535 です。このパラメータが指定されていない場合は、対応する IP アドレスで確立されたすべての SSH 接続が強制的に解放されます。

user-pid *pid-number*:確立された SSH 接続をプロセス番号に基づいて強制的に解放します。pid-number は、解放される SSH 接続プロセス番号で、1~2147483647 の範囲の値を取ります。現在の SSH 接続のプロセス番号は、display ssh server session で確認できます。

username *username*:ユーザ名に基づいて確立された SSH 接続を強制的に解放します。現在の SSH 接続のユーザ名は、display ssh server session で確認できます。

説明

free ssh コマンドは、確立された SSH 接続を強制的に解放するために使用します。

例

#IPv 4 アドレス 192.168.15.45 で確立された SSH 接続を強制的に解放します。

<Sysname> free ssh user-ip 192.168.15.45
Releasing SSH connection.Continue?[Y/N]:y
Releasing SSH connection.Continue?[Y/N]:y

#プロセス番号 417 の SSH 接続を強制的に解放します。

<Sysname> free ssh user-pid 417
Releasing SSH connection.Continue?[Y/N]:y

#ユーザ名 sshuser で確立された SSH 接続を強制的に解放します。

<Sysname> free ssh username sshuser
Releasing SSH connection.Continue?[Y/N]:y

関連コマンド

- **display ssh server session**

6.1.4 sftp server enable

Syntax

sftp server enable

undo sftp server enable

デフォルト

SFTP サーバ機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

sftp server enable コマンドを使用して、SFTP サーバ機能をオンにします。

undo sftp server enable コマンドは、SFTP サーバ機能を停止するために使用します。

例

#SFTP サーバ機能を有効にします。

<Sysname> system-view
[Sysname] sftp server enable

関連コマンド

- **display ssh server**

6.1.5 sftp server idle-timeout

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

デフォルト

SFTP ユーザ接続のアイドルタイムアウトは 10 分です。

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value:タイムアウト時間。1~35791 の値を分単位で指定できます。

説明

sftp server idle-timeout コマンドは、SFTP サーバ側で SFTP ユーザ接続のアイドルタイムアウト時間を設定するために使用します。

undo sftp server idle-timeout コマンドを使用して、デフォルトの状態を復元します。

SFTP ユーザの接続のアイドル時間が設定されたしきい値を超えると、システムはそのユーザの接続を自動的に切断し、ユーザが操作を行わずに長時間接続を消費することを効果的に回避します。同一時間内の同時 SFTP 接続数が多ければ、この値を適切に小さくし、システム資源を解放して新規ユーザにアクセスできるようにする。

例

#SFTP ユーザ接続のアイドルタイムアウトを 500 分に設定します。

<Sysname> system-view
[Sysname] sftp server idle-timeout 500

関連コマンド

- **display ssh server**

6.1.6 ssh server acl

Syntax

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

デフォルト

すべての IPv4 SSH クライアントがデバイスに SSH アクセスを開始できるようにします。

View

System view

定義済みユーザロール

network-admin

パラメータ

advanced-acl-number:IPv 4 拡張 ACL を 3000~3999 の値で指定します。

basic-acl-number:IPv 4 ベース ACL を 2000~2999 の範囲で指定します。

mac *acl-number*:レイヤ 2 ACL を指定します。acl-number はレイヤ 2 ACL の番号で、範囲は 4000~4999 です。

説明

ssh server acl コマンドは、IPv4 SSH クライアントへのアクセス制御を設定するために使用します。

undo ssh server acl コマンドを使用して、デフォルトの状態を復元します。

IPv4 SSH クライアントへのアクセス制御は、次のように ACL を参照することで行われます。

- 参照 ACL が存在しない場合、または参照 ACL が空の場合、IPv4 SSH クライアントはデバイスにアクセスできません。
- 参照 ACL が空でない場合、ACL の permit ルールに一致する IPv4 SSH クライアントだけがデバイスにアクセスでき、他のクライアントはデバイスにアクセスできません。

この設定を有効にすると、新しく確立された SSH 接続のみがフィルタリングされ、確立された SSH 接続には影響しません。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#IPv 4 アドレス 1.1.1.1 の SSH クライアントだけが、デバイスへの SSH アクセスを許可されます。

<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ssh server acl 2001

関連コマンド

- **display ssh server**

6.1.7 ssh server acl-deny-log enable

Syntax

ssh server acl-deny-log enable

undo ssh server acl-deny-log enable

デフォルト

SSH クライアントが ACL でアクセス禁止になった後、ログ情報の印刷機能がオフになります。

View

System view

定義済みユーザロール

network-admin

説明

ssh server acl-deny-log enable コマンドを使用して、SSH クライアントが ACL でアクセス禁止になった後にログ情報を印刷する機能を有効にします。

undo ssh server acl-deny-log enable コマンドを使用して、SSH クライアントが ACL でアクセス禁止になった後にログ情報を出力しないようにします。

この設定を行うと、SSH クライアントが ACL によってアクセス禁止になったときにログ情報が生成されます。生成されたログ情報は機器の情報センタに送られ、情報センタのパラメータを設定することでログ情報の出力ルールを決定する(出力が許可されているかどうかと出力方向)。

例

#SSH クライアントを有効にする ACL でアクセスが禁止されている場合にログ情報を出力する機能。

<Sysname> system-view
[Sysname] ssh server acl-deny-log enable

関連コマンド

- **ssh server acl**

6.1.8 ssh server authentication-retries

Syntax

ssh server authentication-retries *retries*

undo ssh server authentication-retries

デフォルト

SSH ユーザ認証の試行が許可される最大回数は 3 回です。

View

System view

定義済みユーザロール

network-admin

パラメータ

retries:SSH ユーザ認証の最大試行回数を 1~5 の値で指定します。

説明

ssh server authentication-retries コマンドを使用して、SSH ユーザ認証試行を許可する最大回数を設定します。

undo ssh server authentication-retries コマンドを使用して、デフォルトの状態を復元します。

このコマンドを使用すると、ユーザがログインを試行する回数を制限し、不正なユーザによるユーザ名とパスワードの不正な推測やクラッキングを防止できます。

ユーザの認証回数が最大認証回数を超え、まだ認証に成功していない場合、認証は許可されません。認証方式によって認証回数の統計方式が異なります。具体的な統計方式は以下を参考してください:

- any 認証方式では、認証回数は SSH クライアントが publickey と password の両方で認証を試みた回数の合計です。
- password-publickey 認証方式では、アプライアンスは最初に SSH ユーザを publickey 認証し、次に password 認証します。これは、2 回の認証試行ではなく 1 回の認証試行です。

この設定は、すでにログインしている SSH ユーザには影響せず、新しくログインした SSH ユーザにのみ有効です。

例

#SSH ユーザ認証試行を許可する最大回数を 4 に指定します。

<Sysname> system-view
[Sysname] ssh server authentication-retries 4

関連コマンド

- **display ssh server**

6.1.9 ssh server authentication-timeout

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

デフォルト

SSH ユーザの認証タイムアウトは 60 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value:認証タイムアウト時間は、 1120 の範囲で、単位は秒である。

説明

ssh server authentication-timeout コマンドは、SSH サーバ側で SSH ユーザの認証タイムアウト時間を設定します。

undo ssh server authentication-timeout コマンドを使用して、デフォルトの状態を復元します。

SSH ユーザが設定された認証タイムアウト時間内に認証を完了しない場合、SSH サーバはユーザの接続を拒否します。

不正なユーザが TCP 接続を確立した後、次の認証を行わず、システムリソースを占有し、他の正当なユーザの正常なログインを妨げることを防止するために、SSH ユーザ認証タイムアウト時間を適宜調整することができる。

例

#SSH ユーザ認証のタイムアウトを 10 秒に設定します。

<Sysname> system-view
[Sysname] ssh server authentication-timeout 10

関連コマンド

- **display ssh server**

6.1.10 ssh server compatible-ssh1x enable

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [**enable**]

デフォルト

SSH サーバは、SSH 1 バージョンのクライアントと互換性がありません。

View

System view

定義済みユーザロール

network-admin

network-operator

説明

ssh server compatible-ssh1x enable コマンドを使用して、SSH 1 バージョンと互換性のある SSH サーバクライアントを設定します。

undo ssh server compatible-ssh1x [enable]コマンドを使用して、デフォルトを復元します。

この設定は、すでにログインしている SSH ユーザには影響せず、新しくログインした SSH ユーザにのみ有効です。

undo コマンドの実行時に enable を指定した場合も enable を指定しない場合も、デフォルトに戻ります。

例

#SSH 1 バージョンと互換性のあるサーバクライアントを設定して下さい。

<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable

関連コマンド

- **display ssh server**

6.1.11 ssh server dscp

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [**enable**]

デフォルト

IPv4 SSH メッセージの DSCP 優先度は 48 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value:IPv4 SSH メッセージの DSCP 優先度。範囲は 0~63 です。値が大きいほど、優先順位が高くなります。

説明

ssh server dscp コマンドは、IPv4 SSH サーバが SSH クライアントに送信するメッセージの DSCP 優先順位を設定するために使用します。

undo ssh server dscp コマンドを使用して、デフォルトの状態を復元します。

DSCP は IP メッセージ中の ToS フィールドを持ち、メッセージ自体の優先順位を表し、メッセージ転送の優先度を決定する。

例

#IPv4 SSH サーバが SSH クライアントに送信するメッセージの DSCP 優先順位を 30 に設定します。

<Sysname> system-view
[Sysname] ssh server dscp 30

6.1.12 ssh server enable

Syntax

ssh server enable

undo ssh server enable

デフォルト

Stelnet サーバ機能が停止しています。

View

System view

定義済みユーザロール

network-admin

説明

ssh server enable コマンドは、Stelnet サーバ機能を有効にするために使用します。

undo ssh server enable コマンドは、Stelnet サーバ機能を停止するために使用します。

例

#Stelnet サーバ機能を有効にします。

<Sysname> system-view
[Sysname] ssh server enable

関連コマンド

- **display ssh server**

6.1.13 ssh server port

Syntax

ssh server port *port-number*

undo ssh server port

デフォルト

SSH サービスのポート番号は 22 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number:SSH サービスのポート番号。範囲は 1~65535 です。

説明

ssh server port コマンド SSH サービスを構成するために使用されるポート番号。

undo ssh server port コマンドを使用して、デフォルトの状態を復元します。

注意

- ポート番号を変更する前に SSH サービスがオンになっていた場合、ポート番号を変更すると SSH サービスが自動的に再起動され、アクセスしているユーザは切断されます。ユーザがアクセスを続行するには、SSH 接続を再確立する必要があります。
- 1~1024 間の既知のポート番号を使用すると、他のサービスの起動に失敗する可能性があります。

例

#SSH サービスのポート番号を 1025 に設定します。

<Sysname> system-view
[Sysname] ssh server port 1025

6.1.14 ssh server rekey-interval

Syntax

ssh server rekey-interval *interval*

undo ssh server rekey-interval

デフォルト

RSA サーバキーペアの最小更新間隔が 0 の場合、システムは RSA サーバキーペアを更新しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:サーバキーペアの最小更新間隔。1~24 の値を、時間単位で指定します。

説明

ssh server rekey-interval コマンドを使用して、RSA サーバキーペアの最小更新間隔を設定します。

undo ssh server rekey-interval コマンドを使用して、デフォルトの状態を復元します。

サーバのキーペアを定期的に更新することで、キーペアに対する悪意のある推測やクラッキングを防ぐことができ、SSH 接続のセキュリティが向上する。

このコマンドを構成した後、最初の SSH 1 ユーザがログインしてから、SSH サーバは、新しい SSH 1 ユーザがログインするまで待機して、現在の RSA サーバのキーペアを更新し、新しい RSA サーバのキーペアを使用して、新しくログインした SSH 1 ユーザとキーペアのネゴシエーションを行います。最大待機時間は、ここで設定した最小更新間隔です。その後、次の新しい SSH 1 ユーザがログインするまで、この手順を繰り返して RSA サーバキーの更新を再度トリガーしません。

この設定は、SSH クライアントバージョンが SSH 1 のユーザにのみ有効です。

例

#RSA サーバキーペアの最小更新間隔を 3 時間に設定します。

<Sysname> system-view
[Sysname] ssh server rekey-interval 3

関連コマンド

- **display ssh server**

6.1.15 ssh user

Syntax

ssh user *username* **service-type** { **all** | **scp** | **sftp** | **stelnet** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } [**assign** { **pki-domain** *domain-name* | **publickey** *keyname*&<1-6> }] }

undo ssh user *username*

デフォルト

SSH ユーザが存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

username:SSH ユーザ名。1~80 文字の文字列で、大文字と小文字が区別されます。ユーザ名に記号 「¥」 、 「|」 、 「/」 、 「:」 、 「*」 、 「?」 を含めることはできません。」 、 「<」 、 「>」 、 「@」 、 「a」 、 「A」 、「al」、「aL」、「AL」、「アル」、「all」、「aLl」、「aLL」、「すべて」、「ALl」、「ALL」、「alL」、「aLL」 は使用できません。ここで、 「@」 、 「¥」 、および 「/」 は、ユーザ名として pureusername@domain、pureusername/domain、domain¥pureusername の ISP ドメイン名セパレータでのみ使用されます。SCP サービスタイプのユーザを作成するときは、ユーザ名に短い横棒を含めないでください。そうしないと、このユーザ名を使用した SCP ログインは失敗します。

service-type:SSH ユーザのサービスタイプ。内容:

- all:scp、sftp、stelnet の 3 つのサービスタイプがあります。
- scp:サービスタイプは SCP (Secure Copy の略称)です。
- sftp:サービスタイプは SFTP (Secure FTP の略称)。
- stelnet:サービスタイプは Stelnet (Secure Telnet の略称)です。

authentication-type:SSH ユーザの認証方法。内容:

- *password*:ユーザの認証方式を password に強制的に指定します。この認証方式の暗号化メカニズムは簡単で、暗号化速度が速く、AAA (Authentication, Authorization, Accounting,認証、認可、課金)と結合してユーザ認証、許可と課金を実現できるが、攻撃に対して脆弱である。
- *any*:ユーザの認証方式を指定しないで、ユーザは password 認証または publickey 認証のいずれかを使用できます。
- *password-publickey*:クライアントのバージョンが SSH 2 であることを指定するユーザ認証方式は、password と publickey の両方の認証を行う必要があり、セキュリティが強化されています。クライアント版 SSH 1 のユーザ認証方式は、どちらかの認証を行えばよい。
- *publickey*:ユーザの認証方式を publickey に強制的に指定します。この認証方式は暗号化速度が比較的遅いが、認証強度が高く、パスワードを推測する暴挙などの攻撃方式の影響を受けにくく、使いやすさも高い。1 回の構成が成功すると、その後の認証プロセスが自動的に実行されます。ユーザがパスワードを記憶して入力する必要はありません。

assign:クライアントの認証に使用するパラメータを指定します。

- *pki-domain domain-name*:クライアント証明書を検証する PKI ドメインを指定します。domain-name は PKI ドメイン名を表す 1~31 文字の文字列で、大文字と小文字は区別されません。「~」 、「*」 、「¥」 、「|」 、「:」 、「.」 、「<」 、「>、 「」 、 「'」 は使用できません。サーバ側では、この PKI ドメインに保持された CA 証明書を用いてクライアント証明書の正当性チェックを行うため、クライアントの公開鍵をあらかじめ保持する必要がなく、多数のクライアントの認証要求に柔軟に対応できる。
- *publickey keyname& <1-6>*:SSH クライアントの公開鍵を指定します。複数の SSH クライアントの公開鍵を指定できます。keyname は、1~64 文字の文字列で構成されたクライアント公開キー名を表し、大文字と小文字が区別されます。&<1-6>は、前のパラメータが 6 回まで入力できることを示します。サーバ側はあらかじめローカルに保存しておいたユーザの公開鍵を使ってユーザの正当性チェックを行い、クライアント側の鍵ファイルが変更された場合にはサーバ側でローカルの設定を速やかに更新する必要がある。複数のユーザ公開鍵を指定した場合、ユーザがいずれかの公開鍵で認証されていれば、SSH ユーザを認証するときに、指定した公開鍵を使用して構成順に認証されます。

説明

ssh user コマンドを使用して、SSH ユーザを作成し、SSH ユーザのサービスタイプと認証方法を指定します。

SSH ユーザを削除するには、**undo ssh use**r コマンドを使用します。

SSH ユーザの構成は、次のようにサーバ側で使用される認証方式に依存します。

- サーバが publickey 認証を使用する場合は、アプライアンス上に適切な SSH ユーザと、同じ名前のローカルユーザ(次の認証属性で使用:作業ディレクトリ、ユーザの役割)を作成する必要があります。
- サーバが password 認証を使用する場合は、アプライアンス上に適切なローカルユーザ(ローカル認証に適用)を作成するか、リモートサーバ上に適切な SSH ユーザ(リモート認証用の RADIUS サーバなど)を作成する必要があります。この場合、この構成で適切な SSH ユーザを作成する必要はありません。SSH ユーザを作成する場合は、正しいサービス・タイプと認証方法を指定する必要があります。
- サーバが password-publickey または any 認証を使用する場合は、該当する SSH ユーザをアプライアンスに作成し、同じ名前のローカルユーザ(ローカル認証に適用)または同じ名前の SSH ユーザ(リモート認証用の RADIUS サーバなど)をリモート認証サーバに作成する必要があります。

SCP または SFTP ユーザがログインするときに使用する作業ディレクトリは、ユーザが使用する認証方法に依存します。

- publickey または password-publickey 認証を使用するユーザは、対応するローカル User view で authorization-attribute コマンドによって設定された作業ディレクトリを使用します。
- password 認証方式のユーザが使用するワーキングディレクトリは、AAA によって承認されたワーキングディレクトリです。

SSH ユーザがログインするユーザの役割は、ユーザが使用する認証方法に依存します。

- publickey または password-publickey 認証を使用するユーザの役割は、対応するローカルユーザ表示で authorization-attribute コマンドによって設定されたユーザの役割です。
- password 認証を使用するユーザの役割は、AAA によって承認されたユーザの役割です。

このコマンドを使用してユーザに公開鍵または PKI ドメインを指定する場合は、最後に指定した公開鍵または PKI ドメインが優先されます。pki-domain と publickey を指定しない場合は、そのユーザが証明書認証方式でログインし、サーバが所属する PKI ドメインを用いてクライアントの証明書を検証することを意味する。

SSH ユーザ構成の変更は、すでにログインしている SSH ユーザには影響せず、新しくログインしたユーザに対してのみ有効です。

例

#SSH ユーザ user1 を作成し、user1 のサービスタイプを SFTP、認証モードを password-publickey に設定し、クライアントの公開キーを key 1 に指定します。

<Sysname> system-view
[Sysname] ssh user user1 service-type sftp authentication-type password-publickey assign publickey key1

#デバイス管理クラスのローカルユーザを作成 user1、ユーザパスワードをクリアテキストで設定 123456 TESTplat&!、サービスタイプは SSH、許可ワーキングディレクトリは flash:、許可ユーザロールは network-admin です。

[Sysname] local-user user1 class manage
[Sysname-luser-manage-user1] password simple 123456TESTplat&!
[Sysname-luser-manage-user1] service-type ssh
[Sysname-luser-manage-user1] authorization-attribute work-directory flash:user-role network-admin

関連コマンド

- **authorization-attribute (セキュリティ/AAA)**
- **display ssh user-information**
- **local-user (セキュリティ/AAA)**

6.2 SSHクライアント構成コマンド

6.2.1 bye

Syntax

bye

View

SFTP client view

定義済みユーザロール

network-admin

network-operator

説明

bye コマンドを使用して、リモート SFTP サーバへの接続を終了し、User view に戻ります。

このコマンドの機能は、exit、quit と同じです。

例

#リモート SFTP サーバへの接続を終了します。

sftp>bye
<Sysname>

6.2.2 cd

Syntax

cd [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path:インテント作業パスの名前。

説明

cd コマンドは、リモート SFTP サーバ上の作業パスを変更します。

コマンド「cd ..」を使用して、前のレベルのディレクトリに戻ります。

コマンド「cd/」を使用して、システムのルートディレクトリに戻ります。

例

#作業パスを new 1 に変更します。

```
sftp>cd new1
Current Directory is:/new 1
sftp>pwd
Remote working directory:/new 1
sftp>
```

6.2.3 cdup

Syntax

cdup

View

SFTP client view

定義済みユーザロール

network-admin

例

#カレントワーキングディレクトリ/test1 から 1 つ上のディレクトリに戻る。

```
sftp>cd test1
Current Directory is:/test1
sftp>pwd
Remote working directory:/test1
sftp>cdup
Current Directory is:/
```

sftp>pwd
Remote working directory:/
sftp>

6.2.4 delete

Syntax

delete *remote-file*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file:削除するファイルの名前。

説明

delete コマンドは、SFTP サーバで指定されたファイルを削除するために使用します。

このコマンドは **remove** と同じです。

例

#サーバ上のファイル temp.c を削除します。

sftp>delete temp.c
Removing /temp.c

6.2.5 dir

Syntax

dir [**-a** | **-l**] [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

-a:指定したディレクトリ内のファイルおよびフォルダの詳細を、「.」で始まるファイルおよびフォルダの詳細を含むリストとして表示します。

-l:指定されたディレクトリ内のファイルおよびフォルダの詳細をリストとして表示します。 「.」 で始まるファイルおよびフォルダの詳細は表示しません。

remote-path:クエリのディレクトリ名。remote-path が指定されていない場合は、カレントワーキングディレクトリのファイルとフォルダの情報が表示されます。

説明

dir コマンドは、指定したディレクトリ内のファイルとフォルダの情報を表示します。

-a および-l パラメータが指定されていない場合は、指定されたディレクトリにあるファイルおよびフォルダの名前が表示されます。

このコマンドの機能は **ls** と同じです。

例

#現在の作業ディレクトリにあるファイルとフォルダの詳細を、「.」 で始まるファイルとフォルダの詳細を含むリストとして表示します。

sftp>dir -a

drwxrwxrwx2 115 12 Dec 18 14:12.

drwxrwxrwx2 115 12 Dec 18 14:12..

-rwxrwxrwx1 11301 Dec 18 14:11 010.pub

-rwxrwxrwx1 11301 Dec 18 14:12 011.pub

-rwxrwxrwx1 11301 Dec 18 14:12 012.pub

#現在の作業ディレクトリにあるファイルとフォルダの詳細をリストとして表示しますが、 「.」 で始まるファイルとフォルダの詳細は表示しません。

sftp>dir -l

-rwxrwxrwx1 11301 Dec 18 14:11 010.pub

-rwxrwxrwx1 11301 Dec 18 14:12 011.pub

-rwxrwxrwx1 11301 Dec 18 14:12 012.pub

6.2.6 display sftp client source

Syntax

display sftp client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display sftp client source コマンドを使用して、SFTP クライアントの送信元 IP アドレスの設定を表示します。

例

#SFTP クライアントの送信元 IP アドレスの設定を表示します。

<Sysname> display sftp client source

The source IP address of the SFTP client is 192.168.0.1.

The source IPv6 address of the SFTP client is 2:2::2:2.

関連コマンド

- **sftp client source**

6.2.7 display ssh client source

Syntax

display ssh client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ssh client source コマンドは、STelnet クライアントの送信元 IP アドレスの設定を表示するために使用します。

例

#STelnet クライアントの送信元 IP アドレス設定を表示します。

<Sysname> display ssh client source

The source IP address of the SSH client is 192.168.0.1.

The source IPv6 address of the SSH client is 2:2::2:2.

関連コマンド

- **ssh client source**

6.2.8 exit

Syntax

exit

View

SFTP client view

定義済みユーザロール

network-admin

network-operator

説明

exit コマンドを使用して、リモート SFTP サーバへの接続を終了し、User view に戻ります。

このコマンドの機能は、**bye**、**quit** と同じです。

例

#リモート SFTP サーバへの接続を終了します。

sftp>exit

<Sysname>

6.2.9 get

Syntax

get *remote-file* [*local-file*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file:リモート SFTP サーバ上のファイル名。

local-file:ローカルファイル名。ローカルファイル名が指定されていない場合、ローカルに保存されたファイル名はサーバ上のファイル名と同じとみなされます。

説明

get コマンドは、リモート SFTP サーバからファイルをダウンロードし、ローカルに保存するために使用します。

例

#リモートサーバの temp1.c ファイルをダウンロードし、ローカルに temp.c というファイル名で保存します。

```
sftp> get temp1.c temp.c
Fetching /temp1.c to temp.c
/temp.c                                       100% 1424        1.4KB/s    00:00
```

6.2.10 help

Syntax

help

View

SFTP client view

定義済みユーザロール

network-admin

network-operator

説明

help コマンドは、SFTP クライアントコマンドのヘルプ情報を表示します。

入力しますか**?help** コマンドと同じ機能です。

例

#ヘルプを表示します。

```
sftp> help
Available commands:
  bye                                Quit sftp
  cd [path]                          Change remote directory to 'path'
  cdup                               Change remote directory to the parent directory
  delete path                        Delete remote file
  dir [-a|-l][path]                  Display remote directory listing
      -a                             List all filenames
      -l                             List filename including the specific
                                     information of the file
  exit                               Quit sftp
  get remote-path [local-path]       Download file
  help                               Display this help text
  ls [-a|-l][path]                   Display remote directory
      -a                             List all filenames
      -l                             List filename including the specific
```

	information of the file
mkdir path	Create remote directory
put local-path [remote-path]	Upload file
pwd	Display remote working directory
quit	Quit sftp
rename oldpath newpath	Rename remote file
remove path	Delete remote file
rmdir path	Delete remote empty directory
?	Synonym for help

6.2.11 ls

Syntax

ls [**-a** | **-l**] [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

-a:指定したディレクトリ内のファイルおよびフォルダの詳細を、 「.」 で始まるファイルおよびフォルダの詳細を含むリストとして表示します。

-l:指定されたディレクトリ内のファイルおよびフォルダの詳細をリストとして表示します。 「.」 で始まるファイルおよびフォルダの詳細は表示しません。

remote-path:クエリのディレクトリ名。remote-path が指定されていない場合は、カレントワーキングディレクトリのファイルとフォルダの情報が表示されます。

説明

ls コマンドを使用して、指定したディレクトリ内のファイルとフォルダの情報を表示します。

-a および-l パラメータが指定されていない場合は、指定されたディレクトリにあるファイルおよびフォルダの名前が表示されます。

このコマンドの機能は dir と同じです。

例

#現在の作業ディレクトリにあるファイルとフォルダの詳細を、「.」 で始まるファイルとフォルダの詳細を含むリストとして表示します。

sftp>ls -a

drwxrwxrwx2 115 12 Dec 18 14:12.

drwxrwxrwx2 115 12 Dec 18 14:12..

-rwxrwxrwx1 11301 Dec 18 14:11 010.pub

-rwxrwxrwx1 11301 Dec 18 14:12 011.pub

-rwxrwxrwx1 11301 Dec 18 14:12 012.pub

#現在の作業ディレクトリにあるファイルとフォルダの詳細をリストとして表示しますが、 「.」 で始まるファイルとフォルダの詳細は表示しません。

sftp>ls -l

-rwxrwxrwx1 11301 Dec 18 14:11 010.pub

-rwxrwxrwx1 11301 Dec 18 14:12 011.pub

-rwxrwxrwx1 11301 Dec 18 14:12 012.pub

6.2.12 mkdir

Syntax

mkdir *remote-path*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path:リモート SFTP サーバ上のディレクトリ名。

説明

mkdir コマンドを使用して、リモート SFTP サーバに新しいディレクトリを作成します。

例

#リモート SFTP サーバにディレクトリ test を作成します。

sftp>mkdir test

6.2.13 put

Syntax

put *local-file* [*remote-file*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

local-file:ローカルファイル名。

remote-file:リモート SFTP サーバ上のファイル名。リモートサーバ上のファイル名が指定されていない場合、サーバ上に保存されているファイル名はローカルファイル名と同じとみなされます。

説明

put コマンドを使用して、ローカルファイルをリモート SFTP サーバにアップロードします。

例

#ローカル startup.bak ファイルをリモート SFTP サーバにアップロードし、startup01.bak ファイル名で保存します。

sftp>put startup.bak startup01.bak
Uploading startup.bak to /startup01.bak
startup01.bak100% 14241.4 KB/秒 00:00

6.2.14 pwd

Syntax

pwd

View

SFTP client view

定義済みユーザロール

network-admin

説明

pwd コマンドを使用して、リモート SFTP サーバ上の現在の作業ディレクトリを表示します。

例

#リモート SFTP サーバの現在の作業ディレクトリを表示します。

sftp>pwd
Remote working directory:/

上記の情報は、現在の作業ディレクトリがルートディレクトリであることを示しています。

6.2.15 quit

Syntax

quit

View

SFTP client view

定義済みユーザロール

network-admin

network-operator

説明

quit コマンドを使用して、リモート SFTP サーバへの接続を終了し、User view に戻ります。

このコマンドの機能は、**bye**、**exit** と同じです。

例

#リモート SFTP サーバへの接続を終了します。

sftp>quit
<Sysname>

6.2.16 remove

Syntax

remove *remote-file*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file:削除するファイルの名前。

説明

remove コマンドは、リモート SFTP サーバで指定されたファイルを削除するために使用します。

このコマンドは、**delete** コマンドと同じです。

例

#リモート SFTP サーバ上のファイル temp.c を削除します。

sftp>remove temp.c
Removing /temp.c

6.2.17 rename

Syntax

rename *old-name new-name*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

old-name:元のファイル名またはフォルダ名。

new-name:新しいファイル名またはフォルダ名。

説明

rename コマンドは、リモート SFTP サーバで指定されたファイルまたはフォルダの名前を変更します。

例

#リモート SFTP サーバ上のファイル temp1.c の名前を temp2.c に変更します。

sftp>dir
aa.pubtemp1.c
sftp>rename temp1.c temp2.c
sftp>dir
aa.pubtemp2.c

6.2.18 rmdir

Syntax

rmdir *remote-path*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path:リモート SFTP サーバ上のディレクトリ名。

説明

rmdir コマンドは、リモート SFTP サーバで指定されたディレクトリを削除するために使用します。

例

#SFTP サーバの現在の作業ディレクトリにある temp1 ディレクトリを削除します。

sftp>rmdir temp1

6.2.19 sftp

Syntax

sftp *server* [*port-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server:サーバの IPv 4 アドレスまたはホスト名。1~253 文字の文字列で、大文字と小文字は区別されません。

port-number:サーバのポート番号。範囲は 1~65535 で、デフォルト値は 22 です。

identity-key:クライアント publickey が認証に使用する公開鍵アルゴリズム。デフォルトは dsa です。サーバが publickey 認証を使用する場合は、このパラメータを指定する必要があります。クライアントは、指定されたアルゴリズムのローカル秘密鍵を使用して、デジタル署名または証明書を生成します。

- *dsa*:公開鍵アルゴリズムは DSA である。
- *ecdsa-sha2-nistp256*:公開鍵長 256 の ECDSA アルゴリズムを指定します。
- *ecdsa-sha2-nistp384*:公開鍵長 384 の ECDSA アルゴリズムを指定します。
- *rsa*:公開鍵アルゴリズムは RSA である。
- *x509v3-ecdsa-sha2-nistp256*:x509v3-ecdsa-sha2-nistp256 公開鍵アルゴリズム。
- *x509v3-ecdsa-sha2-nistp384*:x509v3-ecdsa-sha2-nistp384 公開鍵アルゴリズム。
- *pki-domain domain-name*:クライアント証明書の PKI ドメインを、大文字と小文字を区別しない 1~31 文字の文字列で指定します。公開鍵アルゴリズムが x509v3 の場合は、クライアント証明書が存在する PKI ドメイン名を指定して、正しいローカル証明書を取得します。

prefer-compress:サーバとクライアント間の圧縮アルゴリズム。デフォルトではサポートされていません。

zlib:圧縮アルゴリズム ZLIB。

prefer-ctos-cipher:クライアントからサーバへの優先暗号化アルゴリズム。デフォルトは aes128-ctr です。des-cbc、3 des-cbc、aes128-cbc、aes128-ctr、aes128-gcm、aes192-ctr、aes256-cbc、aes256-ctr、aes256-gcm アルゴリズムのセキュリティ強度と計算にかかる時間は、順に増加します。

- *3 des-cbc*:3 DES-CBC 暗号化アルゴリズム。
- *aes128-cbc*:128 ビット AES-CBC 暗号化アルゴリズム。
- *aes128-ctr*:128 ビット AES-CTR 暗号化アルゴリズム。
- *aes128-gcm*:128 ビット AES-GCM 暗号化アルゴリズム。
- *aes192-ctr*:192 ビット AES-CTR 暗号化アルゴリズム。
- *aes256-cbc*:256 ビット AES-CBC 暗号化アルゴリズム。
- *aes256-ctr*:256 ビット AES-CTR 暗号化アルゴリズム。
- *aes256-gcm*:256 ビット AES-GCM 暗号化アルゴリズム。
- *des-cbc*:DES-CBC 暗号化アルゴリズム。

prefer-ctos-hmac:クライアントからサーバへの優先 HMAC アルゴリズム。デフォルトは sha2-256 です。md 5、md5-96、sha 1、sha1-96、sha2-256、sha2-512 アルゴリズムのセキュリティ強度と計算にかかる時間は、順に増加します。

- *md 5*:HMAC アルゴリズム HMAC-MD5。
- *md5-96*:HMAC アルゴリズム HMAC-MD5-96。
- *sha 1*:HMAC アルゴリズム HMAC-SHA1。
- *sha1-96*:HMAC アルゴリズム HMAC-SHA1-96。
- *sha2-256*:HMAC アルゴリズム HMAC-SHA2-256。
- *sha2-512*:HMAC アルゴリズム HMAC-SHA2-512。

prefer-kex:鍵交換の優先アルゴリズム。デフォルトは ecdh-sha2-nistp256 です。dh-group-exchange-sha1、dh-group1-sha1、dh-group14-sha1、ecdh-sha2-nistp256、ecdh-sha2-nistp384 アルゴリズムのセキュリティ強度と処理にかかる時間は、順に増加します。

- *dh-group-exchange-sha1*:鍵交換アルゴリズム diffie-hellman-group-exchange-sha1。
- *dh-group1-sha1*:鍵交換アルゴリズム diffie-hellman-group1-sha1。
- *dh-group14-sha1*:鍵交換アルゴリズム diffie-hellman-group14-sha1。

- *ecdh-sha2-nistp256*:鍵交換アルゴリズム ecdh-sha2-nistp256。
- *ecdh-sha2-nistp384*:鍵交換アルゴリズム ecdh-sha2-nistp384。

prefer-stoc-cipher:サーバ側からクライアント側への優先暗号化アルゴリズム。デフォルトは aes128-ctr です。サポートされている暗号化アルゴリズムは、クライアントからサーバへの暗号化アルゴリズムと同じです。

prefer-stoc-hmac:サーバ側からクライアント側への優先 HMAC アルゴリズム。デフォルトは sha2-256 です。サポートされる暗号化アルゴリズムは、クライアントからサーバへの HMAC アルゴリズムと同じです。

dscp dscp-value:クライアントが送信する SFTP メッセージに含まれる DSCP の優先度を 0~63 の範囲で指定します。デフォルト値は 48 です。DSCP は IP メッセージ中の ToS フィールドを持ち、メッセージ自体の優先順位を表し、メッセージ転送の優先度を決定する。

public-key keyname:サーバ側の ID を検証するサーバ側のホスト公開鍵を指定します。ここで、keyname は、すでに構成されているホストの公開鍵の名前で、大文字と小文字を区別しない 1~64 文字の文字列です。

server-pki-domain *domain-name*:サービス側証明書を検証する PKI ドメインを指定します。ここで、domain-name は認証サービス側証明書の PKI ドメイン名を表し、1~31 文字の文字列です。大文字と小文字は区別されず、「~」、「*」、「¥」、「|」、「:」、「.」、「<」、「>、「」、「'」は使用できません。

source:サーバと通信する送信元 IPv 4 アドレスまたは送信元インタフェースを指定します。デフォルトでは、メッセージの送信元 IPv 4 アドレスは、ルーティングテーブルのエントリに基づいて検索され、このメッセージを送信したアウトバウンドインタフェースのプライマリ IPv 4 アドレスです。指定されたインタフェースで障害が発生してもクライアントとサーバ間の通信が中断されないようにするには、通常、送信元インタフェースとして Loopback インタフェース、または送信元 IPv 4 アドレスとして Loopback インタフェース、Dialer インタフェースの IPv 4 アドレスを指定することをお勧めします。

interface *interface-type interface-number*:送信元インタフェースを指定します。interface-type interface-number はインターフェイスタイプおよびインタフェース番号です。システムは、このインタフェースのプライマリ IPv 4 アドレスを送信元 IP アドレスとして使用します。

ip *ip-address*:送信元 IPv 4 アドレスを指定します。

説明

sftp コマンドを使用して、リモート IPv4 SFTP サーバとの接続を確立し、SFTP client view に入ります。

クライアントホストの公開鍵アルゴリズムが証明書として正常にネゴシエートされると、サービス側証明書が正しいことを確認する必要があります。正しい認証サーバ証明書を取得するには、server-pki-domain でサービス側証明書の PKI ドメイン名を指定する必要があります。クライアントは、その PKI ドメインに保存されている CA 証明書を用いてサーバ証明書の正当性チェックを行い、サーバの公開鍵をあらかじめ保存しておく必要

はない。クライアントが認証サービス側証明書が存在する PKI ドメインを指定しない場合、認証にはデフォルトでクライアント証明書が存在するPKI ドメインが使用されます。

例

#SFTP クライアントは、 publickey 認証方式で IP アドレス 10.1.1.2 の SFTP サーバに接続し、次のような接続ポリシーを用いてサーバ側の公開鍵名を svkey と指定する.

- 優先鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先 HMAC アルゴリズムは sha 1 です。
- サーバからクライアントへの HMAC アルゴリズムは sha1-96 です。
- サーバとクライアント間の圧縮アルゴリズムは zlib が推奨されます。

<Sysname> sftp 10.1.1.2 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey

6.2.20 sftp client source

Syntax

sftp client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo sftp client source

デフォルト

SFTP クライアントが使用する送信元 IPv 4 アドレスが設定されていません。SFTP クライアントが SFTP メッセージを送信するために使用する送信元 IPv 4 アドレスは、ルーティングテーブルエントリに基づいて検出された、このメッセージを送信するアウトバウンドインタフェースのプライマリ IP アドレスです。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*:送信元アドレスとしてインタフェースのプライマリ IP アドレスを指定します。interface-type interface-number は、送信元インターフェイスタイプと送信元インタフェース番号を示します。

ip *ip-address*:送信元 IP アドレスを指定します。

説明

sftp client source コマンドを使用して、SFTP クライアントが SFTP メッセージを送信するために使用する送信元 IPv 4 アドレスを設定します。

undo sftp client source コマンドを使用して、デフォルトの状態を復元します。

sftp client source コマンドで指定された送信元アドレスはすべての SFTP 接続で有効であり、**sftp** コマンドで指定された送信元アドレスは現在の SFTP 接続でのみ有効です。

このコマンドでソースアドレスを指定した後、 SFTP ユーザが **sftp** コマンドでログインした際にソースアドレスを指定した場合は、 **sftp** コマンドで指定したソースアドレスを用いる。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#SFTP クライアントが SFTP メッセージを送信するために使用する送信元 IP アドレスを 192.168.0.1 に指定します。

<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1

関連コマンド

- **display sftp client source**

6.2.21 ssh client source

Syntax

ssh client source { **interface** *interface-type interface-number* | **ip** *ip-address* }

undo ssh client source

デフォルト

Stelnet クライアントが使用するソース IPv 4 アドレスが設定されていません。Stelnet クライアントが SSH メッセージを送信するソース IPv 4 アドレスデバイスのルーティングに指定された SSH メッセージアウトインターフェイスのプライマリ IP アドレス。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*:送信元アドレスとしてインタフェースのプライマリ IP アドレスを指定します。interface-type interface-number は、送信元インターフェイスタイプと送信元インタフェース番号を示します。

ip *ip-address*:送信元 IPv 4 アドレスを指定します。

説明

ssh client source コマンドは、Stelnet クライアントが SSH メッセージを送信するために使用する送信元 IPv 4 アドレスを設定します。

undo ssh client source コマンドを使用して、デフォルトの状態を復元します。

ssh client source コマンドで指定された送信元アドレスは、すべての Stelnet 接続で有効です。**ssh 2** コマンドで指定された送信元アドレスは、現在の Stelnet 接続でのみ有効です。

このコマンドを使用してソースアドレスを指定した後、**ssh 2** コマンドを使用して SSH ユーザがログインするときにソースアドレスを指定すると、**ssh 2** コマンドで指定したソースアドレスが使用されます。

このコマンドを複数回実行すると、最後に実行したコマンドが有効になります。

例

#Stelnet クライアントが SSH メッセージを送信するために使用する送信元 IPv 4 アドレスが 192.168.0.1 であることを指定します。

<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1

関連コマンド

- **display ssh client source**

6.2.22 ssh 2

Syntax

ssh2 *server* [*port-number*] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** *domain-name* } | **prefer-compress zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** *dscp-value* | **escape** *character* | { **public-key** *keyname* | **server-pki-domain** *domain-name* } | **source** { **interface** *interface-type interface-number* | **ip** *ip-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server:サーバの IPv 4 アドレスまたはホスト名。1~253 文字の文字列で、大文字と小文字は区別されません。

port-number:サーバのポート番号。範囲は 1~65535 で、デフォルト値は 22 です。

identity-key:クライアント publickey が認証に使用する公開鍵アルゴリズム。デフォルトは dsa です。サーバが publickey 認証を使用する場合は、このパラメータを指定する必要があります。クライアントは、指定されたアルゴリズムのローカル秘密鍵を使用して、デジタル署名または証明書を生成します。

- *dsa*:公開鍵アルゴリズムは DSA である。
- *ecdsa-sha2-nistp256*:公開鍵長 256 の ECDSA アルゴリズムを指定します。
- *ecdsa-sha2-nistp384*:公開鍵長 384 の ECDSA アルゴリズムを指定します。
- *rsa*:公開鍵アルゴリズムは RSA である。
- *x509v3-ecdsa-sha2-nistp256*:x509v3-ecdsa-sha2-nistp256 公開鍵アルゴリズム。
- *x509v3-ecdsa-sha2-nistp384*:x509v3-ecdsa-sha2-nistp384 公開鍵アルゴリズム。
- **pki-domain** *domain-name*:クライアント証明書の PKI ドメインを、大文字と小文字を区別しない 1~31 文字の文字列で指定します。公開鍵アルゴリズムが x509v3 の場合は、クライアント証明書が存在する PKI ドメイン名を指定して、正しいローカル証明書を取得します。

prefer-compress:サーバとクライアント間の圧縮アルゴリズム。デフォルトではサポートされていません。

zlib:圧縮アルゴリズム ZLIB。

prefer-ctos-cipher:クライアントからサーバへの優先暗号化アルゴリズム。デフォルトは aes128-ctr です。des-cbc、3 des-cbc、aes128-cbc、aes128-ctr、aes128-gcm、aes192-ctr、aes256-cbc、aes256-ctr、aes256-gcm アルゴリズムのセキュリティ強度と計算にかかる時間は、順に増加します。

- *3 des-cbc*:3 DES-CBC 暗号化アルゴリズム。
- *aes128-cbc*:128 ビット AES-CBC 暗号化アルゴリズム。
- *aes128-ctr*:128 ビット AES-CTR 暗号化アルゴリズム。
- *aes128-gcm*:128 ビット AES-GCM 暗号化アルゴリズム。
- *aes192-ctr*:192 ビット AES-CTR 暗号化アルゴリズム。
- *aes256-cbc*:256 ビット AES-CBC 暗号化アルゴリズム。
- *aes256-ctr*:256 ビット AES-CTR 暗号化アルゴリズム。
- *aes256-gcm*:256 ビット AES-GCM 暗号化アルゴリズム。
- *des-cbc*:DES-CBC 暗号化アルゴリズム。

prefer-ctos-hmac:クライアントからサーバへの優先 HMAC アルゴリズム。デフォルトは sha2-256 です。md 5、md5-96、sha 1、sha1-96、sha2-256、sha2-512 アルゴリズムのセキュリティ強度と計算にかかる時間は、順に増加します。

- *md 5*:HMAC アルゴリズム HMAC-MD5。
- *md5-96*:HMAC アルゴリズム HMAC-MD5-96。
- *sha 1*:HMAC アルゴリズム HMAC-SHA1。
- *sha1-96*:HMAC アルゴリズム HMAC-SHA1-96。
- *sha2-256*:HMAC アルゴリズム HMAC-SHA2-256。
- *sha2-512*:HMAC アルゴリズム HMAC-SHA2-512。

prefer-kex:鍵交換の優先アルゴリズム。デフォルトは ecdh-sha2-nistp256 です。dh-group-exchange-sha1、dh-group14-sha1、ecdh-sha2-nistp256、ecdh-sha2-nistp384 アルゴリズムのセキュリティ強度と計算にかかる時間は、順に増加します。

- *dh-group-exchange-sha1*:鍵交換アルゴリズム diffie-hellman-group-exchange-sha1。
- *dh-group1-sha1*:鍵交換アルゴリズム diffie-hellman-group1-sha1。
- *dh-group14-sha1*:鍵交換アルゴリズム diffie-hellman-group14-sha1。
- *ecdh-sha2-nistp256*:鍵交換アルゴリズム ecdh-sha2-nistp256。
- *e*cdh-sha2-nistp384:鍵交換アルゴリズム ecdh-sha2-nistp384。

prefer-stoc-cipher:サーバ側からクライアント側への優先暗号化アルゴリズム。デフォルトは aes128-ctr です。サポートされている暗号化アルゴリズムは、クライアントからサーバへの暗号化アルゴリズムと同じです。

prefer-stoc-hmac:サーバ側からクライアント側への優先 HMAC アルゴリズム。デフォルトは sha2-256 です。サポートされる暗号化アルゴリズムは、クライアントからサーバへの HMAC アルゴリズムと同じです。

dscp *dscp-value*:クライアントが送信する SFTP メッセージに含まれる DSCP の優先度を 0~63 の範囲で指定します。デフォルト値は 48 です。DSCP は IP メッセージ中の ToS フィールドを持ち、メッセージ自体の優先順位を表し、メッセージ転送の優先度を決定する。

escape *character*:終了文字を指定します。character は大文字と小文字が区別される 1 文字で、デフォルトは~です。つまり、~.と入力すると、サーバから強制的に切断されます。

public-key *keyname*:サーバ側の ID を検証するサーバ側のホスト公開鍵を指定します。ここで、keyname は、すでに構成されているホストの公開鍵の名前で、大文字と小文字を区別しない 1~64 文字の文字列です。

server-pki-domain *domain-name*:サービス側証明書を検証する PKI ドメインを指定します。ここで、domain-name は認証サービス側証明書の PKI ドメイン名を表し、1~31 文字の文字列です。大文字と小文字は区別されず、 「~」 、 「*」 、 「¥」 、 「|」 、 「:」 、 「.」 、 「<」 、 「>、 「」 、 「'」 は使用できません。

source:サーバと通信する送信元 IPv 4 アドレスまたは送信元インタフェースを指定します。デフォルトでは、メッセージの送信元 IPv 4 アドレスは、ルーティングテーブルのエントリに基づいて検索され、このメッセージを送信したアウトバウンドインタフェースのプライマリ IPv 4 アドレスです。指定したインタフェースで障害が発生してもクライアントとサーバ間の通信が中断されないようにするには、通常、送信元インタフェースとして Loopback インタフェース、または送信元アドレスとして Loopback インタフェース、Dialer インタフェースの IPv 4 アドレスを指定することをお勧めします。

interface *interface-type interface-number*:送信元インタフェースを指定します。interface-type interface-number はインターフェイスタイプおよびインタフェース番号です。システムは、このインタフェースのプライマリ IPv 4 アドレスを送信元 IP アドレスとして使用します。

ip *ip-address*:送信元 IPv 4 アドレスを指定します。

説明

ssh 2 コマンドを使用して、Stelnet クライアントと IPv4 Stelnet サーバ側の接続を確立します。

クライアントホストの公開鍵アルゴリズムが証明書として正常にネゴシエートされると、サービス側証明書が正しいことを確認する必要があります。正しい認証サーバ証明書を取得するには、server-pki-domain でサービス側証明書の PKI ドメイン名を指定する必要があります。クライアントは、その PKI ドメインに保存されている CA 証明書を用いてサーバ証明書の正当性チェックを行い、サーバの公開鍵をあらかじめ保存しておく必要はない。クライアントが認証サービス側証明書が存在する PKI ドメインを指定しない場合､認証にはデフォルトでクライアント証明書が存在するPKIドメインが使用されます。

終了文字の使用については、次の点に注意してください。

- 終了文字と文字.を使用すると、クライアントとサーバの接続を強制的に切断できます(これは通常、サーバ側の再起動や例外が発生した場合に、クライアントが現在の接続を迅速に切断するために使用されます。)。
- このアクションを有効にするには、行に終了文字と.を入力する必要があります。行に別の文字を入力したことがあるか､別のアクション(例えば退格)を実行した場合は、行を折り返す必要があります。
- 一般に、ログアウト文字と.の組み合わせがログインユーザ名と同じにならないように、デフォルトの終了文字を使用することをお勧めします。

例

#Stelnet クライアントは､publickey 認証を使用して､アドレス 3.3.3.3 のリモート Stelnet サーバにログインし、次の接続ポリシーを使用して、サーバ側の公開キー名を svkey に指定します。

- 優先鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先 HMAC アルゴリズムは sha 1 です。
- サーバからクライアントへの HMAC アルゴリズムは sha1-96 です。
- サーバとクライアントの間の優先圧縮アルゴリズムは zlib です。
- $.を入力すると、クライアントとサービス側の接続が強制的に切断されます。

<Sysname> ssh 2 3.3.3.3 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey escape $

6.3 SSH 2プロトコル構成コマンド

6.3.1 display ssh2 algorithm

Syntax

display ssh2 algorithm

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ssh2 algorithm コマンドは、アプライアンスで設定されている SSH 2 プロトコルで使用されているアルゴリズムの優先リストを表示します。

例

#デバイスで設定されている SSH 2 プロトコルで使用されるアルゴリズムの優先順位のリストを表示します。

<Sysname> display ssh2 algorithm

Key exchange algorithms:ecdh-sha2-nistp256 ecdh-sha2-nistp384 dh-group-exchange-sha1 dh-group14-sha1 dh-group1-sha1

Public key algorithms:ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 rsa dsa

Encryption algorithms:aes128-ctr aes192-ctr aes256-ctr aes128-gcm aes256-gcm aes128-cbc 3des-cbc aes256-cbc des-cbc

MAC algorithms:sha2-256 sha2-512 sha1 md5 sha1-96 md5-96

表 6-4 display ssh2 algorithm コマンドの表示情報の説明

フィールド	説明
Key exchange algorithms	現在使用されているキー交換アルゴリズムのリストを優先度順に表示します。
Public key algorithms	現在使用されているホストアルゴリズムのリストを優先度順に表示します。
Encryption algorithms	現在使用されている暗号化アルゴリズムのリストを優先度順に表示します
MAC algorithms	現在使用されているHMACアルゴリズムのリストを優先度順に表示します。

関連コマンド

- **ssh2 algorithm key-exchange**
- **ssh2 algorithm public-key**
- **ssh2 algorithm cipher**
- **ssh2 algorithm mac**

6.3.2 ssh2 algorithm cipher

Syntax

ssh2 algorithm cipher { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } *

undo ssh2 algorithm cipher

デフォルト

SSH 2 プロトコルで使用されるデフォルトの暗号化アルゴリズムの優先順位は、aes128-ctr、aes192-ctr、aes256-ctr、aes128-gcm、aes256-gcm、aes128-cbc、3 des-cbc、aes256-cbc、および des-cbc です。

View

System view

定義済みユーザロール

network-admin

パラメータ

3 des-cbc:3 DES-CBC 暗号化アルゴリズム。

aes128-cbc:128 ビット AES-CBC 暗号化アルゴリズム。

aes128-ctr:128 ビット AES-CTR 暗号化アルゴリズム。

aes128-gcm:128 ビット AES-GCM 暗号化アルゴリズム。

aes192-ctr:192 ビット AES-CTR 暗号化アルゴリズム。

aes256-cbc:256 ビット AES-CBC 暗号化アルゴリズム。

aes256-ctr:256 ビット AES-CTR 暗号化アルゴリズム。

aes256-gcm:256 ビット AES-GCM 暗号化アルゴリズム。

des-cbc:DES-CBC 暗号化アルゴリズム。

説明

ssh2 algorithm cipher コマンドを使用して、SSH 2 プロトコルで使用される暗号化アルゴリズムのリストを設定します。

undo ssh2 algorithm cipher コマンドを使用して、デフォルトの状態を復元します。

このコマンドを使用すると、特定の暗号化アルゴリズムのみを使用するように SSH 2 がデバイスの動作環境で要求されている場合に、デバイス上の SSH 2 クライアントおよび SSH 2 サーバで使用できる暗号化アルゴリズムを構成の範囲内に制限できます。アルゴリズムが配置される順序は、アルゴリズムの優先順位です。

例

#SSH 2 プロトコルで使用する暗号化アルゴリズムを aes256-cbc に設定します。

<Sysname> system-view
[Sysname] ssh2 algorithm cipher aes256-cbc

関連コマンド

- **display ssh2 algorithm**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

6.3.3 ssh2 algorithm key-exchange

Syntax

ssh2 algorithm key-exchange { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } *

undo ssh2 algorithm key-exchange

デフォルト

SSH 2 プロトコルで使用されるデフォルトのキー交換アルゴリズムは、ecdh-sha2-nistp256、ecdh-sha2-nistp384、dh-group-exchange-sha1、dh-group14-sha1、および dh-group1-sha1 の優先度の高い順にリストされます。

View

System view

定義済みユーザロール

network-admin

パラメータ

dh-group-exchange-sha1:鍵交換アルゴリズム diffie-hellman-group-exchange-sha1。

dh-group1-sha1:鍵交換アルゴリズム diffie-hellman-group1-sha1。

dh-group14-sha1:鍵交換アルゴリズム diffie-hellman-group14-sha1。

ecdh-sha2-nistp256:鍵交換アルゴリズム ecdh-sha2-nistp256。

ecdh-sha2-nistp384:鍵交換アルゴリズム ecdh-sha2-nistp384。

説明

ssh2 algorithm key-exchange コマンドを使用して、SSH 2 プロトコルで使用されるキー交換アルゴリズムのリストを設定します。

undo ssh2 algorithm key-exchange コマンドを使用して、デフォルトの状態を復元します。

このコマンドを使用すると、SSH 2 が特定のキー交換アルゴリズムのみを使用する必要があるデバイス実行環境で、SSH 2 クライアントおよび SSH 2 サーバで使用できるキー

交換アルゴリズムを設定の範囲内に制限できます。アルゴリズムが配置される順序は、アルゴリズムの優先順位です。

例

#SSH 2 プロトコルで使用するキー交換アルゴリズムを dh-group1-sha1 に設定します。

<Sysname> system-view
[Sysname] ssh2 algorithm key-exchange dh-group1-sha1

関連コマンド

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm mac**
- **ssh2 algorithm public-key**

6.3.4 ssh2 algorithm mac

Syntax

ssh2 algorithm mac { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } *

undo ssh2 algorithm mac

デフォルト

SSH 2 プロトコルで使用されるデフォルトの HMAC アルゴリズムは、優先度の高い順に sha2-256、sha2-512、sha 1、md 5、sha1-96、md5-96 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

md 5:HMAC アルゴリズム HMAC-MD5。

md5-96:HMAC アルゴリズム HMAC-MD5-96。

sha 1:HMAC アルゴリズム HMAC-SHA1。

sha1-96:HMAC アルゴリズム HMAC-SHA1-96。

sha2-256:HMAC アルゴリズム HMAC-SHA2-256。

sha2-512:HMAC アルゴリズム HMAC-SHA2-512。

説明

ssh2 algorithm mac コマンドを使用して、SSH 2 プロトコルで使用される HMAC アルゴリズムのリストを設定します。

undo ssh2 algorithm mac コマンドを使用して、デフォルトの状態を復元します。

このコマンドは、SSH 2 が特定の HMAC アルゴリズムのみを使用できることがデバイスの動作環境で必要とされる場合に、デバイス上の SSH 2 クライアントおよび SSH 2 サーバが使用できる HMAC アルゴリズムを構成の範囲内に制限するために使用します。アルゴリズムが配置される順序は、アルゴリズムの優先順位です。

例

#SSH 2 プロトコルの設定で使用される HMAC アルゴリズムは md 5 です。

<Sysname> system-view
[Sysname] ssh2 algorithm mac md5

関連コマンド

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm public-key**

6.3.5 ssh2 algorithm public-key

Syntax

ssh2 algorithm public-key { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** } *

undo ssh2 algorithm public-key

デフォルト

SSH 2 プロトコルで使用されるデフォルトのホスト署名アルゴリズムは、ecdsa-sha2-nistp256、ecdsa-sha2-nistp384、rsa、および dsa の優先度の高いリストです。

View

System view

定義済みユーザロール

network-admin

パラメータ

dsa:公開鍵アルゴリズムは DSA である。

ecdsa-sha2-nistp256:公開鍵長 256 の ECDSA アルゴリズムを指定します。

ecdsa-sha2-nistp384:公開鍵長 384 の ECDSA アルゴリズムを指定します。

rsa:公開鍵アルゴリズムは RSA である。

説明

ssh2 algorithm public-key コマンドを使用して、SSH 2 プロトコルで使用されるホスト署名アルゴリズムのリストを設定します。

undo ssh2 algorithm public-key コマンドを使用して、デフォルトの状態を復元します。

アプライアンスの実行環境で、特定のホスト署名アルゴリズムのみを使用する SSH 2 が必要な場合は、このコマンドを使用して、アプライアンス上の SSH 2 クライアントおよび SSH 2 サーバが使用できるホスト署名アルゴリズムを構成の範囲内に制限できます。アルゴリズムが配置される順序は、アルゴリズムの優先順位です。

例

#SSH 2 プロトコルの構成に使用されるホスト署名アルゴリズムは dsa です。

<Sysname> system-view
[Sysname] ssh2 algorithm public-key dsa

関連コマンド

- **display ssh2 algorithm**
- **ssh2 algorithm cipher**
- **ssh2 algorithm key-exchange**
- **ssh2 algorithm mac**

目次

このセクションのページは **15-x-x** です。

7 章 SSL 7-1
7.1 SSL 設定コマンド 7-1
7.1.1 certificate-chain-sending enable 7-1
7.1.2 display ssl client-policy 7-2
7.1.3 display ssl server-policy 7-3
7.1.4 pki-domain (SSL client policy view) 7-5
7.1.5 pki-domain (SSL server policy view) 7-6
7.1.6 server-verify enable 7-7
7.1.7 ssl client-policy 7-8
7.1.8 ssl server-policy 7-9
7.1.9 ssl version disable 7-10
7.1.10 version 7-11

7章 SSL

7.1 SSL設定コマンド

7.1.1 certificate-chain-sending enable

Syntax

certificate-chain-sending enable

undo certificate-chain-sending enable

デフォルト

SSL ネゴシエーションの実行中、SSL サーバは、完全な証明書チェーンではなくサーバ証明書をクライアントに送信します。

View

SSL server policy view

定義済みユーザロール

network-admin

説明

certificate-chain-sending enable コマンドは SSL ネゴシエーションの実行中に SSL サーバが完全な証明書チェーンをクライアントに送信できるようにします。

undo certificate-chain-sending enable コマンドはデフォルトに戻します。

この機能により、SSL ネゴシエーションプロセスで追加の処理が発生します。SSL クライアントがサーバ証明書を確認するための完全な証明書チェーンを持っていない場合のみ、有効にします。

例

SSL サーバが SSL ネゴシエーションの実行中に完全な証明書チェーンをクライアントに送信できるようにします。

<AP> system-view

[AP] ssl server-policy policy1

[AP-ssl-server-policy-policy1] certificate-chain-sending enable

7.1.2 display ssl client-policy

Syntax

display ssl client-policy [*policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy-name： SSL クライアントポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。このパラメータを省略した場合、すべての SSL クライアントポリシーに関する情報を表示します。

説明

display ssl client-policy コマンドは、指定された SSL クライアントポリシーまたはすべての SSL クライアントポリシーについての情報を表示します。

例

SSL クライアントポリシーpolicy1 についての情報を表示します。

<AP> display ssl client-policy policy1

```
SSL Client Policy: policy1
    SSL version: TLS 1.0
    PKI domain:
    Preferred ciphersuite:
        DHE_RSA_AES_256_CBC_SHA
        RSA_AES_256_CBC_SHA
        DHE_RSA_AES_128_CBC_SHA
        RSA_AES_128_CBC_SHA
        RSA_3DES_EDE_CBC_SHA
    Server-verify: enabled
```

表7-1 コマンド出力

フィールド	説明
SSL Client Policy	SSLクライアントポリシー名です。

フィールド	説明
SSL version	SSLクライアントポリシーで使用するSSLプロトコルのバージョンです。 • SSL3.0 • TLS1.0 • TLS1.1 • TLS1.2
PKI Domain	SSLクライアントポリシーに使用されるPKIドメインです。
Preferred ciphersuite	SSLクライアントポリシーに使用される暗号スイートの優先順位です。
Server-verify	SSLクライアントが、デジタル証明書を使用してサーバを認証するかを示します。

7.1.3 display ssl server-policy

Syntax

display ssl server-policy [*policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy-name： SSL サーバポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。このパラメータを省略した場合、すべての SSL サーバポリシーに関する情報を表示します。

説明

display ssl server-policy コマンドは、指定された SSL サーバポリシーまたはすべての SSL サーバポリシーについての情報を表示します。

例

SSL サーバポリシーpolicy1 についての情報を表示します。

<AP> display ssl server-policy policy1

```
SSL server policy: policy1
    Version info:
```

```
    SSL3.0: Disabled
    TLS1.0: Enabled
    TLS1.1: Disabled
    TLS1.2: Enabled
    TLS1.3: Disabled
PKI domains: server-domain
Ciphersuites:
    DHE_RSA_AES_128_CBC_SHA
    RSA_AES_128_CBC_SHA
Session cache size: 600
Caching timeout: 3600 seconds
Client-verify: Enabled
Ciphersuite server-perferred: Disabled
```

表7-2 コマンド出力

フィールド	説明
SSL Server Policy	SSLサーバポリシー名です。
Version info	SSLサーバポリシーで使用するSSLプロトコルのバージョンです。SSLサーバは、有効になっているSSLプロトコルバージョンでのみ、セッションネゴシエーションを行います。 • **SSL3.0** • **TLS1.0** • **TLS1.1** • **TLS1.2** • **TLS1.3**
PKI Domain	SSLサーバポリシーに使用されるPKIドメインです。
Ciphersuite	SSLサーバポリシーにサポートされる暗号スイートです。
Session Timeout	SSLサーバポリシーのセッションタイムアウト時間です(秒) 。
Caching timeout	SSLサーバポリシーのセッションキャッシュタイムアウト時間です(秒)。
Client-verify	デジタル証明書を使用してSSLクライアントを認証するかを示します。 • **Disabled**－クライアント認証は無効。 • **Enabled**－クライアント認証は必須。 • **Optimal**－クライアント認証は任意。

フィールド	説明
Ciphersuite server-perferred	SSLサーバとSSLクライアント間の暗号スイートネゴシエーションで、サーバの優先順位使用の状態を示します。 • **Enabled**－サーバの暗号スイート優先順位を使用します。 • **Disabled**－クライアントの暗号スイート優先順位を使用します。

7.1.4 pki-domain (SSL client policy view)

Syntax

pki-domain *domain-name*

undo pki-domain

デフォルト

設定なし

View

SSL client policy view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。

説明

pki-domain コマンドは、SSL サーバポリシーまたは SSL クライアントポリシーの PKI ドメインを指定します。

undo pki-domain コマンドは、デフォルトに戻します。

SSL クライアントポリシーに PKI ドメインを指定すると、SSL クライアントポリシーを使用する SSL クライアントは、指定された PKI ドメインを介してデジタル証明書を取得します。

例

SSL クライアントポリシー **policy1** に、PKI ドメイン **client-domain** を設定します。

<AP> system-view

[AP] ssl client-policy policy1

[AP-ssl-client-policy-policy1] pki-domain client-domain

関連コマンド

- **display ssl client-policy**
- **display ssl server-policy**

7.1.5 pki-domain (SSL server policy view)

Syntax

pki-domain *domain-name&<1-2>*

undo pki-domain

デフォルト

設定なし

View

SSL server policy view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。*&<1-2>*は、1 つまたは 2 つの PKI ドメインを指定する必要があることを表します。

説明

pki-domain コマンドは、SSL サーバポリシーまたは SSL クライアントポリシーの PKI ドメインを指定します。

undo pki-domain コマンドは、デフォルトに戻します。

SSL サーバポリシーに PKI ドメインを指定すると、SSL サーバポリシーを使用する SSL サーバは、指定された PKI ドメインを介してデジタル証明書を取得します。

一部のサービス (ロードバランシングやプロキシポリシーなど) では、サーバ上で 2 つのデジタル証明書を使用する必要がある場合があります。要件を満たすために、このコマンドを使用して、SSL サーバポリシーに一度に 2 つの PKI ドメインを指定できます。指定した PKI ドメインの 2 つのデジタル証明書が異なるタイプの公開キーアルゴリズムを使用していることを確認します。同じタイプの公開キーアルゴリズムを使用している場合は、最初の PKI ドメインによって取得されたデジタル証明書だけが有効になります。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

SSL サーバポリシー **policy1** に、PKI ドメイン **server-domain** を設定します。

<AP> system-view

[AP] ssl server-policy policy1

[AP-ssl-server-policy-policy1] pki-domain server-domain

関連コマンド

- **display ssl client-policy**
- **display ssl server-policy**

7.1.6 server-verify enable

Syntax

server-verify enable

undo server-verify enable

デフォルト

有効

View

SSL client policy view

定義済みユーザロール

network-admin

説明

server-verify enable コマンドは、デジタル証明書を使用した SSL サーバの認証を有効にします。

undo server-verify enable コマンドはデジタル証明書を使用した SSL サーバの認証を無効にします。

この機能により、SSL クライアントは、デジタル証明書を使用して SSL サーバを認証します。SSL サーバの認証を有効にする場合、SSL サーバは認証のためにデジタル証明書を SSL クライアントに送信する必要があります。SSL クライアントは、サーバが認証に合格した後にのみ、SSL サーバへアクセスできます。

例

SSL クライアントが、デジタル証明書を使用して SSL サーバを認証できるようにします。

<AP> system-view

[AP] ssl client-policy policy1

[AP-ssl-client-policy-policy1] server-verify enable

関連コマンド

display ssl client-policy

7.1.7 ssl client-policy

Syntax

ssl client-policy *policy-name*

undo ssl client-policy *policy-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name： SSL クライアントポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。

説明

ssl client-policy コマンドは、SSL クライアントポリシーを作成しその view へ移行するか、既存の SSL クライアントポリシーの view へ移行します。

undo ssl client-policy コマンドは、指定された SSL クライアントポリシー、またはすべての SSL クライアントポリシーを削除します。

SSL クライアントポリシーには、クライアントがサーバへの接続を確立するための使用する SSL パラメータを設定します。パラメータには、PKI ドメイン、優先暗号スイートが含まれます。

SSL クライアントポリシーがアプリケーションに関連付けられている場合、SSL クライアントポリシーを削除することはできません。

例

SSL クライアントポリシー **policy1** を作成し、その view へ移行します。

<AP> system-view

[AP] ssl client-policy policy1

[AP-ssl-client-policy-policy1]

関連コマンド

display ssl client-policy

7.1.8 ssl server-policy

Syntax

ssl server-policy *policy-name*

undo ssl server-policy *policy-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name： SSL サーバポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。

説明

ssl server-policy コマンドは、SSL サーバポリシーを作成しその view へ移行するか、既存の SSL サーバポリシーの view へ移行します。

undo ssl server-policy コマンドは、指定された SSL サーバポリシー、またはすべての SSL サーバポリシーを削除します。

SSL サーバポリシーがアプリケーションに関連付けられている場合、SSL サーバポリシーを削除することはできません。

例

SSL サーバポリシーpolicy1 を作成し、その view へ移行します。

<AP> system-view

[AP] ssl server-policy policy1

[AP-ssl-server-policy-policy1]

関連コマンド

display ssl server-policy

7.1.9 ssl version disable

⚠ **注意:**

SSL Version 設定を変更する場合、**ssl version disable** コマンドあるいは **undo ssl version disable** コマンドを設定したのち、HTTPS サービスを有効にする必要があります。すでに HTTPS サービスが有効である場合、無効にした後、再度有効にしてください。

Syntax

ssl version { **ssl3.0 | tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** } **disable**

undo ssl version { **ssl3.0 | tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** } **disable**

デフォルト

SSL3.0、TLS1.0、TLS1.1、TLS1.2、TLS1.3 が有効。

View

System view

定義済みユーザロール

network-admin

パラメータ

ssl3.0: SSL3.0 を指定します。

tls1.0: TLS1.0 を指定します。

tls1.1: TLS1.1 を指定します。

tls1.2: TLS1.2 を指定します。

tls1.3: TLS1.3 を指定します。

説明

ssl version disable コマンドは SSL サーバがセッションネゴシエーションに特定の SSL プロトコルバージョンを使用しないようにします。

undo ssl version disable コマンドはデフォルトに戻します。

システムセキュリティを強化するために、SSL サーバがセッションネゴシエーションに 特定の SSL プロトコルバージョン(SSL3.0、TLS1.0、TLS1.1、TLS1.2 および TLS1.3) を使用しないよう にすることができます。

例

装置で SSL 3.0 を無効にします。

<AP> system-view

[AP] ssl version ssl3.0 disable

7.1.10 version

Syntax

version { **ssl3.0 | tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** }

undo version { **ssl3.0 | tls1.0** | **tls1.1** | **tls1.2** | **tls1.3** }

デフォルト

SSL クライアントポリシーでは、SSL プロトコルバージョン TLS1.0 を使用します。

View

SSL client policy view

定義済みユーザロール

network-admin

パラメータ

ssl3.0: SSL3.0 を指定します。

tls1.0: TLS1.0 を指定します。

tls1.1: TLS1.1 を指定します。

tls1.2: TLS1.2 を指定します。

tls1.3: TLS1.3 を指定します。

説明

version コマンドは SSL クライアントポリシーで使用する SSL プロトコルバージョンを指定します。

undo version コマンドはデフォルトに戻します。

システムセキュリティを強化するため、SSL プロトコルバージョンに SSL3.0 を指定しないでください。

このコマンドを複数回実行すると、最後に設定した内容が有効になります。

例

SSL クライアントポリシー **policy1** の SSL プロトコルバージョンに TLS1.0 を設定します。

<AP> system-view

[AP] ssl client-policy policy1

[AP-ssl-client-policy-policy1] version tls1.0

目次

このセクションのページは **15-x-x** です。

8 章 接続制限 8-1
8.1 接続制限設定コマンド 8-1
8.1.1 connection-limit 8-1
8.1.2 connection-limit apply 8-2
8.1.3 connection-limit apply global 8-3
8.1.4 description 8-3
8.1.5 display connection-limit 8-4
8.1.6 display connection-limit statistics 8-7
8.1.7 display connection-limit stat-nodes 8-8
8.1.8 limit 8-10
8.1.9 reset connection-limit statistics 8-12

8章 接続制限

8.1 接続制限設定コマンド

8.1.1 connection-limit

Syntax

connection-limit { **policy** } *policy-id*

undo connection-limit { **policy** } *policy-id*

デフォルト

接続数制限ポリシーがありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

policy:IPv4 接続数制限ポリシーを指定します。

policy-id:接続数制限ポリシー番号(接続数制限ポリシーの番号空間はそれぞれ独立である.)。範囲は 1~32 です。

説明

connection-limit コマンドを使用して、接続数制限ポリシーを作成し、ビューに移動します。指定した接続数制限ポリシーがすでに存在する場合は、ビューに直接移動します。

undo connection-limit コマンドは、接続数制限ポリシーを削除するために使用します。

例

#番号 1 の IPv4 接続数制限ポリシーを作成し、ビューに移動します。

<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1]

関連コマンド

- **connection-limit apply**
- **connection-limit apply global**
- **display connection-limit**

- **limit**

8.1.2 connection-limit apply

Syntax

connection-limit apply { **policy** } *policy-id*

undo connection-limit apply { **policy** }

デフォルト

インタフェースに接続数制限ポリシーが適用されていません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

policy:IPv4 接続数制限ポリシーを指定します。

policy-id:接続数制限ポリシー番号。範囲は 1~32 です。

説明

connection-limit apply コマンドを使用して、インタフェースに接続数制限ポリシーを適用します。

undo connection-limit apply コマンドを使用して、インタフェースに適用された接続数制限ポリシーをキャンセルします。

1 つのインタフェースに適用できる IPv 4 接続制限ポリシーは 1 つだけです。新しい IPv 4 接続制限ポリシーは、古いものを上書きします。

例

#インタフェース Vlan-interface2 に番号 1 の IPv4 接続数制限ポリシーを適用します。

<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] connection-limit apply policy 1

関連コマンド

- **connection-limit**
- **limit**

8.1.3 connection-limit apply global

Syntax

connection-limit apply global { **policy** } *policy-id*

undo connection-limit apply global { **policy** }

デフォルト

グローバル未適用接続数制限ポリシー

View

System view

定義済みユーザロール

network-admin

パラメータ

policy:IPv4 接続数制限ポリシーを指定します。

policy-id:接続数制限ポリシー番号。範囲は 1~32 です。

説明

connection-limit apply global コマンドは、接続数制限ポリシーをグローバルに適用するために使用します。

undo connection-limit apply global コマンドを使用して、グローバルに適用された接続数制限ポリシーをキャンセルします。

グローバルに適用できるのは、1 つの IPv 4 接続制限ポリシーは 1 つだけです。新しい IPv 4 接続制限ポリシーは、古いものを上書きします。

例

#番号 1 の IPv4 接続数制限ポリシーをグローバルに適用します。

<Sysname> system-view
[Sysname] connection-limit apply global policy 1

関連コマンド

- **connection-limit**
- **limit**

8.1.4 description

Syntax

description *text*

undo description

デフォルト

説明情報が設定されていません。

View

IPv4 connection limit policy view

定義済みユーザロール

network-admin

パラメータ

text:接続数制限ポリシーの説明を示す 1~127 文字の文字列で、大文字と小文字が区別されます。

説明

description コマンド接続数制限ポリシーを設定するために使用される説明情報。

undo description コマンドを使用して、デフォルトの状態を復元します。

description コマンドを使用すると、現在の接続数制限ポリシーにプロファイル情報がない場合は、プロファイル情報が追加されます。それ以外の場合は、既存のプロファイル情報が変更されます。

例

#設定番号 1 の IPv4 接続数制限ポリシーの説明情報は CenterToA です。

<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connlmt-policy-1] description CenterToA

関連コマンド

- **display connection-limit**

8.1.5 display connection-limit

Syntax

display connection-limit { **policy** } { *policy-id* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy:IPv4 接続数制限ポリシーを表示します。

policy-id:接続数制限ポリシー番号。範囲は 1~32 です。

all:指定したタイプのすべての接続数制限ポリシーを表示します。

説明

display connection-limit コマンドは、接続数制限ポリシーの設定情報を表示するために使用します。

例

#すべての IPv4 接続数制限ポリシーの構成情報を表示します。

<Sysname> display connection-limit policy all

```
3 policies in total:
 Policy  Rule    Stat Type  HiThres  LoThres  ACL
--------------------------------------------------------------------------------
     0     1  Src-Dst-Port    2000     1800  3000
          12      Src-Dst     500       45  3001
         255           --  1000000   980000  2001

     1     2     Dst-Port     800       70  3010
           3      Src-Dst     100       90  3000
          10  Src-Dst-Port      50       45  3003
          11          Src     200      200  3004
         200           --   500000   498000  2002

    28     4         Port    1500     1400  3100
           5          Dst    3000      280  3101
          21      Src-Dst     200      180  3102
          25     Src-Port      50       35  3200
Description list:
 Policy     Description
--------------------------------------------------------------------------------
     1      IPv4Description1
    28     Description for IPv4 28
```

#番号 1 の IPv4 接続ポリシーの構成情報を表示します。

<Sysname> display connection-limit policy 1

```
IPv4 connection limit policy 1 has been applied 5 times, and has 5 limit rules.
Description: IPv4Description1
Limit rule list:
 Policy  Rule    Stat Type  HiThres  LoThres  ACL
--------------------------------------------------------------------------------
```

```
     1     2      Dst-Port      800      700  3010
           3       Src-Dst     100       90  3000
          10  Src-Dst-Port       50       45  3003
          11           Src     200      200  3004
         200            --  500000   498000  2002
Application list:
   GigabitEthernet1/0/1
   GigabitEthernet1/0/2
   Vlan-interface1
   Tunnel0
   Global
```

表 8-1 display connection-limit コマンドの表示情報の説明

フィールド	説明
Limit rule list	接続数制限ポリシー情報リスト
Policy	接続数制限ポリシー番号
Rule	接続数制限ルール番号
Stat Type	統計的には、次のような値を取ります。 • Src-Dst-Port:ソース IP-宛先 IP-サービスの組み合わせによる統計と制限 • Src-Dst:送信元 IP と宛先 IP の組み合わせによる統計と制限 • Src-Port:ソース IP-サービスの組み合わせによる統計と制限 • Dst-Port:目的別 IP-サービスの組み合わせの統計と制限 • Src:ソース IP 別の統計と制限 • Dst:宛先 IP 別の統計と制限 • Port:サービス別の統計と制限 • Dslite:DS-Lite トンネルの B 4 デバイス別の統計情報と制限 • --:特定の IP アドレス、サービスに基づいて統計的に制限するのではなく、このルールで参照される ACL に一致するすべての接続は、全体的に指定されたしきい値によって制限されます。
HiThres	最大接続数
LoThres	最低接続数
ACL	ルールが参照するACL番号またはACL名
Application list	接続数制限ポリシー適用リストには、インタフェース名とGlobalが含まれます。ここで、Globalは、グローバルに適用される接続数制限ポリシーを示します。
Description	接続数制限ポリシーの説明
Description list	接続数制限ポリシーの説明情報リスト

関連コマンド

- **connection-limit**
- **connection-limit apply**
- **connection-limit apply global**
- **limit**

8.1.6 display connection-limit statistics

Syntax

display connection-limit statistics { **global** | **interface** *interface-type interface-number* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global:グローバルな接続数制限の統計を表示します。

interface interface-type interface-number:指定したインタフェースの接続数制限の統計情報を表示します。interface-type interface-number はインタフェースのタイプとインタフェース番号を示します。

説明

display connection-limit statistics コマンドは、グローバルまたはインタフェースの接続数制限の統計情報を表示するために使用します。

例

#グローバル接続数制限の統計を表示します。

<Sysname> display connection-limit statistics global

```
Connection limit statistics (Global、slot 1):
Dropped IPv4 packets:54781
Dropped IPv6 packets:11457
```

表 8-2 display connection-limit statistics コマンドの表示情報の説明

フィールド	説明
Dropped IPv4 packet	グローバルまたはインタフェースのIPv4接続数制限ポリシーに一致し、指定された最大接続数を超えたためにドロップされたメッセージの数

フィールド	説明
Dropped IPv6 packet	グローバルまたはインタフェースのIPv6接続数制限ポリシーに一致し、指定された最大接続数を超えたためにドロップされたメッセージの数

関連コマンド

- **connection-limit**
- **connection-limit apply**
- **connection-limit apply global**
- **limit**

8.1.7 display connection-limit stat-nodes

Syntax

display connection-limit stat-nodes { **global** | **interface** *interface-type interface-number* } [**destination** *destination-ip* | **service-port** *port-number* | **source** *source-ip*] * [**count**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global:IPv4 統計ノードのグローバルリストを表示します。

interface *interface-type interface-number*:指定されたインタフェースの IPv4 統計情報ノードのリストを表示します。interface-type interface-number はインタフェースのタイプとインタフェース番号を示します。

destination *destination-ip*:指定された宛先 IP アドレスの IPv4 統計情報ノードのリストを表示します。

service-port *port-number*:指定したサービスポート番号の IPv4 統計情報ノードのリストを表示します。

source *source-ip*:指定した送信元 IP アドレスの IPv4 統計情報ノードのリストを表示します。

count:IPv4 統計ノードの数を表示します。このパラメータを構成すると、条件を満たす (count の前のパラメータによって決定されます。) IPv4 統計ノードの数のみが表示され、IPv4 統計ノードの詳細は表示されません。このパラメーターを指定しない場合、条件に一致する IPv4 統計情報ノードの詳細が表示されます。

説明

display connection-limit stat-nodes コマンドを使用して、グローバルまたはインタフェースに制限された接続数を持つ IPv4 統計情報ノードのリストを表示します。

統計ノードは、接続のメッセージ特性(送信元/宛先 IP アドレス、サービスポート番号、トランスポート・レイヤ・プロトコル・タイプなど)、接続に適用される接続制限ポリシー、現在の接続数の統計値、および新規接続の作成が現在許可されているかどうかを含む、接続数制限の統計および制限を行うオブジェクト(1 つの接続または接続のクラス)を識別する。

source、destination、service-port の 1 つ以上のパラメータを指定すると、統計ノードのリストが複数の条件で表示されます。たとえば、source と destination を指定すると、指定した送信元 IP アドレスと宛先 IP アドレスの両方に一致する統計ノードのリストが表示されます。

source、destination、service-port のいずれのパラメータも指定しない場合は、すべての統計ノードのリストが表示されます。

接続数制限ポリシーを変更または削除しても、そのポリシーによって生成され、すでに有効になっている接続数制限の統計ノードは影響を受けません。これらのノードは、カウントされた接続が切断されると自動的に削除されます。

例

#グローバル IPv4 接続数制限統計ノードの数を表示します。

<Sysname> display connection-limit stat-nodes global count

```
Current limit statistic nodes count is 5.
```

#インタフェース Vlan-interface2 の IPv4 接続制限統計ノードのリストを表示します。

<Sysname> display connection-limit stat-nodes interface vlan-interface 2

```
Src IP address         : 100.100.100.100
    VPN instance       : 01234567890123456789012345678901
 Dst IP address        : 200.200.200.200
    VPN instance       : abcdefghijklmnopqrstuvwxyzabcde
 DS-Lite tunnel peer    : 1234567890
 Service               : tcp/12345
 Limit rule ID         : 12345(ACL: 3001)
 Sessions threshold Hi/Lo: 1100000/980000
 Sessions count        : 1050000
 New session flag      : Permit
```

表 8-3 display connection-limit stat-nodes コマンドの表示情報の説明

フィールド	説明
Src IP address	ソースIPアドレス
Dst IP address	宛先IPアドレス

フィールド	説明
VPN instance	アドレスが属するMPLS L3VPNのインスタンス名「--」は、どのインスタンスにも属していないことを示します。
DS-Lite tunnel peer	一時的にサポートされていないDS Liteトンネル「--」は、どのDS Lite Tunnelにも属していないことを示します。
Service	プロトコル名とサービスポート番号。よく知られていないプロトコルの場合は「unknown (xx)」と表示され、xxはプロトコル番号で、サービスポート番号は表示されません。ただし、ICMPプロトコルの場合、括弧内の数字はICMPのtypeフィールドとcodeフィールドの組み合わせで表される16進数に対応する十進数である
Limit rule ID	一致したACL番号を括弧で囲んだ一致したルール番号
Sessions threshold Hi/Lo	接続数制限の上限値および下限値
Sessions count	現在の接続数
New session flag	新規接続の作成が許可されているかどうか、作成が許可されている場合はPermit、作成が許可されていない場合はDeny 🕮 メモ : 接続数が上限値(max-amount)に達すると、New session flagはPermitとして表示されますが、この時点では新しい接続を作成できません。接続数が上限値を超えた場合のみ、New session flagはDenyとして表示されます。

関連コマンド

- **connection-limit policy**
- **connection-limit apply global policy**
- **connection-limit apply policy**
- **limit**

8.1.8 limit

Syntax

limit *limit-id* **acl** { *acl-number* | **name** *acl-name* } [**per-destination** | **per-service** | **per-source**] * **amount** *max-amount min-amount* [**description** *text*]

undo limit *limit-id*

デフォルト

コネクション数制限ルールは存在しない。

View

IPv4 connection limit policy view

定義済みユーザロール

network-admin

パラメータ

limit-id:コネクション数制約ルール番号であり、 1~256 の値をとる。

acl:ユーザ範囲を照合する ACL を指定します。接続制限ルールは、ACL ルールに一致するユーザ接続の数のみをカウントし、制限します。

*acl-numbe*r:ACL の番号。範囲は 2000~3999 です。

name *acl-name*:ACL の名前。1~63 文字の文字列で、大文字と小文字は区別されません。a~z または A~Z で始まる必要があります。混乱を避けるため、ACL の名前に英語の all を使用することはできません。

per-destination:宛先アドレス別の統計と制限を示します。

per-service:サービス別(トランスポート・レイヤ・プロトコルおよびサービスポート別)の統計と制限を示します。

per-source:送信元アドレスによる統計と制限を示します。

max-amount:接続数の上限を 1~4294967295 の範囲で指定します。接続の範囲またはタイプがこの値を超えると、ユーザは新しい接続を確立できません。

min-amount:接続数の下限を指定します。範囲は 1~4294967295 で、max-amount より大きい値は指定できません。接続数の統計値がこの値を下回ると、ユーザは新しい接続を確立できます。

説明

limit コマンドを使用して、接続数制限ルールを設定します。

undo limit コマンドは、指定された接続数制限ルールを削除するために使用します。

接続数制限ポリシーごとに複数のルールを定義できます。各ルールでは、参照 ACL、ルールのタイプ、および統計的な上限と下限を指定します。タイプが per-destination、per-source、per-service の場合は、1 つのルールで 1 つを個別に指定するか、それらの組み合わせを指定できます。たとえば、per-destination と per-source の両方を指定すると、接続のメッセージ送信元アドレスと宛先アドレスに基づいて統計的に制限され、同じ送信元と宛先を持つ接続は、指定したしきい値によって数が制限される同じクラスの接続に属します。

デバイス上で確立された接続が接続数制限ポリシーに一致すると、一致するルールが見つかるまで、そのポリシー内のすべてのルールがルール番号の小さい順に走査されます。

同じ接続数制限ポリシー内の異なるルールは、異なる ACL を参照する必要があります。

参照 ACL の内容が変更されると、デバイスは新しい接続数制限ポリシーに従って既存の接続を再カウントし、制限します。

per-destination、per-service、per-source の 3 つのパラメータが指定されていない場合、このルールで参照される ACL に一致するすべての接続は、指定されたしきい値によって全体的に制限されます。

例

#IPv 4 接続数制限ポリシー1 では、ルール番号 1 で ACL 3000 を参照し、ACL 3000 に一致する接続をメッセージの送信元アドレスと宛先アドレスで統計的に制限するルールを作成します。接続数の上限は 2000、下限は 1800 です。このルールは、192.168.0.0/24 ネットワークセグメントの各ホストが同時に送信できる接続数を、エクストラネットの同じ宛先 IP アドレスに対して最大 2000 に制限します。2000 を超えると、新しい接続が許可される前に、接続数が 1800 を下回ります。

<Sysname> system-view

[Sysname] acl advanced 3000

[Sysname-acl-ipv4-adv-3000] rule permit ip source 192.168.0.0 0.0.0.255

[Sysname-acl-ipv4-adv-3000] quit

[Sysname] connection-limit policy 1

[Sysname-connlmt-policy-1] limit 1 acl 3000 per-destination per-source amount 2000 1800

関連コマンド

- connection-limit
- display connection-limit

8.1.9 reset connection-limit statistics

Syntax

reset connection-limit statistics { **global** | **interface** *interface-type interface-number* }

View

User view

定義済みユーザロール

network-admin

network-operator

パラメータ

global:グローバルな接続数制限統計をクリアします。

interface *interface-type interface-number*:指定したインタフェースの接続数制限の統計情報をクリアします。interface-type interface-number はインターフェイスタイプとインタフェース番号を示します。

説明

reset connection-limit statistics コマンドを使用して、グローバルまたはインタフェースの接続数制限の統計情報をクリアします。

例

#指定したインタフェース Vlan-interface2 の接続数制限の統計情報をクリアします。

<Sysname> reset connection-limit statistics interface vlan-interface 2

関連コマンド

- **display connection-limit statistics**

目次

このセクションのページは **15-x-x** です。

9 章 TCP フラグメントアタックプロテクション 9-1
9.1 TCP フラグメントアタックプロテクション設定コマンド 9-1
9.1.1 attack-defense tcp fragment enable 9-1

9章 TCP フラグメントアタックプロテクション

9.1 TCPフラグメントアタックプロテクション設定コマンド

9.1.1 attack-defense tcp fragment enable

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

attack-defense tcp fragment enable コマンドを使用すると、TCP フラグメントアタックを防ぐことができます。

undo attack-defense tcp fragment enable コマンドは、TCP フラグメントアタックプロテクション機能を無効にするために使用します。

このコマンドは、パケットフィルタが検出できない TCP フラグメントアタックを防ぐために、デバイスが TCP フラグメントアタックパケットをドロップできるようにします。RFC 1858 で定義されているように、TCP アタックフラグメントパケットとは次の TCP フラグメントパケットを指します。

- TCP ヘッダーが 20 バイトより小さい最初のフラグメントパケット
- フラグメントオフセットが 8 バイト (FO=1) の最初以外のフラグメントパケット

TCP フラグメントアタックプロテクションは、シングルパケットアタックプロテクションよりも優先されます。両方使用する場合、受信した TCP パケットは、最初に TCP フラグメントアタックプロテクションで処理され、次にシングルパケットアタックプロテクションで処理されます。

例

#TCP フラグメントアタックプロテクション機能を有効にします。

<Sysname> system-view

[Sysname] attack-defense tcp fragment enable

目次

このセクションのページは **15-x-x** です。

10 章 IP ソースガード 10-1
10.1 パスワード管理設定コマンド 10-1
10.1.1 ip verify source 10-1

10章 IP ソースガード

10.1 パスワード管理設定コマンド

10.1.1 ip verify source

Syntax

ip verify source

undo ip verify source

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

ip verify source コマンドはスタティックとダイナミックの両方の IPv4 ソースガード機能を有効にします。

undo ip verify source コマンドはスタティックとダイナミックの両方の IPv4 ソースガード機能を無効にします。

この機能は、WLAN スヌーピングエントリを使用して、AP が受信する IPv4 パケットをフィルタリングします。エントリと一致しないパケットはドロップされます。WLAN スヌーピングエントリは、IP-MAC バインディングです。

IPv4 ネットワークでは、IPSG は DHCP パケットによって取得された WLAN スヌーピングエントリのみを使用します。

例

IPv4 ソースガード機能を有効にします。

<Switch> system-view

[Switch] wlan service-template security

[Switch--wlan-st-security] ip verify source

目次

このセクションのページは **15-x-x** です。

11 章 ARP アタックプロテクション 11-1
11.1 ARP IP メッセージアタックプロテクション設定コマンド 11-1
11.1.1 arp resolving-route enable 11-1
11.1.2 arp resolving-route probe-count 11-1
11.1.3 arp resolving-route probe-interval 11-2
11.1.4 arp source-suppression enable 11-3
11.1.5 arp source-suppression limit 11-4
11.1.6 display arp source-suppression 11-5
11.2 ARP メッセージ速度制限設定コマンド 11-5
11.2.1 arp rate-limit 11-5
11.2.2 arp rate-limit log enable 11-6
11.2.3 arp rate-limit log interval 11-7
11.2.4 snmp-agent trap enable arp 11-8
11.3 送信元 MAC アドレス固定 ARP アタック検出設定コマンド 11-9
11.3.1 arp source-mac 11-9
11.3.2 arp source-mac aging-time 11-10
11.3.3 arp source-mac exclude-mac 11-11
11.3.4 arp source-mac threshold 11-12
11.3.5 display arp source-mac 11-13
11.4 ARP メッセージ送信元 MAC アドレスの整合性チェック設定コマンド 11-14
11.4.1 arp valid-check enable 11-14
11.5 ARP プロアクティブ確認設定コマンド 11-14
11.5.1 arp active-ack enable 11-14
11.6 ARP アタック検知設定コマンド 11-15
11.6.1 arp detection enable 11-15
11.6.2 arp detection trust 11-16
11.6.3 arp detection validate 11-17
11.6.4 arp restricted-forwarding enable 11-18
11.6.5 display arp detection 11-18
11.6.6 display arp detection statistics attack-source 11-19
11.6.7 display arp detection statistics packet-drop 11-21
11.6.8 reset arp detection statistics attack-source 11-22
11.6.9 reset arp detection statistics packet-drop 11-22
11.7 ARP 自動スキャン、プロファイリング設定コマンド 11-23
11.7.1 arp scan 11-23

11章 ARP アタックプロテクション

11.1 ARP IPメッセージアタックプロテクション設定コマンド

11.1.1 arp resolving-route enable

Syntax

arp resolving-route enable

undo arp resolving-route enable

デフォルト

ARP ブラックホールルーティング機能がオンになっています。

View

System view

定義済みユーザロール

network-admin

説明

arp resolving-route enable コマンドを使用して、ARP ブラックホールルーティング機能を有効にします。

undo arp resolving-route enable コマンドは、ARP ブラックホールルーティング機能を無効にするために使用されます。

ゲートウェイデバイスでこの機能をオンにすることをお勧めします。

例

#ARP ブラックホールルーティング機能を有効にします。

<Sysname> system-view
[Sysname] arp resolving-route enable

関連コマンド

- **arp resolving-route probe-count**
- **arp resolving-route probe-interval**

11.1.2 arp resolving-route probe-count

Syntax

arp resolving-route probe-count *count*

undo arp resolving-route probe-count

デフォルト

ARP 要求メッセージを送信した回数は 3 回である。

View

System view

定義済みユーザロール

network-admin

パラメータ

count:ARP 要求メッセージが送信された回数。範囲は 1~25 です。

説明

arp resolving-route probe-count コマンドを使用して、ARP 要求メッセージを送信する回数を設定します。

undo arp resolving-route probe-count コマンドを使用して、デフォルトの状態を復元します。

例

#ARP 要求メッセージを 5 回送信するように設定します。

<Sysname> system-view
[Sysname] arp resolving-route probe-count 5

関連コマンド

- **arp resolving-route enable**
- **arp resolving-route probe-interval**

11.1.3 arp resolving-route probe-interval

Syntax

arp resolving-route probe-interval *interval*

undo arp resolving-route probe-interval

デフォルト

ARP 要求メッセージが送信される間隔は 1 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:ARP 要求メッセージを送信する間隔。1~5 の範囲の値を秒単位で指定します。

説明

arp resolving-route probe-interval コマンドを使用して、ARP 要求メッセージを送信する間隔を設定します。

undo arp resolving-route probe-interval コマンドを使用して、デフォルトの状態を復元します。

例

#ARP 要求メッセージを送信する間隔を 3 秒に設定します。

<Sysname> system-view
[Sysname] arp resolving-route probe-interval 3

関連コマンド

- **arp resolving-route enable**
- **arp resolving-route probe-count**

11.1.4 arp source-suppression enable

Syntax

arp source-suppression enable

undo arp source-suppression enable

デフォルト

ARP 送信元アドレス抑制機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

arp source-suppression enable コマンドを使用して、ARP 送信元アドレス抑制機能を有効にします。

undo arp source-suppression enable コマンドを使用して、ARP 送信元アドレス抑制機能を無効にします。

ゲートウェイデバイスでこの機能をオンにすることをお勧めします。

例

#ARP 送信元アドレス抑制機能を有効にします。

<Sysname> system-view
[Sysname] arp source-suppression enable

関連コマンド

- **display arp source-suppression**

11.1.5 arp source-suppression limit

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

デフォルト

ARP ソース抑制のしきい値は 10 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

limit-value:ARP 送信元抑制のしきい値。5 秒間隔でデバイスが処理できる送信元 IP は同じですが、宛先 IP アドレスで解決できない IP メッセージの最大数。範囲は 2~1024 です。

説明

arp source-suppression limit コマンドを使用して、ARP ソース抑制のしきい値を設定します。

undo arp source-suppression limit コマンドを使用して、デフォルトの状態を復元します。

IP アドレスからデバイスのインタフェースに送信される宛先 IP アドレスが解決できない IP メッセージが、ネットワーク内で 5 秒ごとに設定されたしきい値を超えた場合、デバイスは 5 秒が経過するまで IP アドレスから送信された IP メッセージを処理しなくなり、悪意のある攻撃による被害を回避できます。

例

#ARP ソース抑制のしきい値を 100 に設定します。

<Sysname> system-view
[Sysname] arp source-suppression limit 100

関連コマンド

- **display arp source-suppression**

11.1.6 display arp source-suppression

Syntax

display arp source-suppression

View

すべての view

定義済みユーザロール

network-admin
network-operator

説明

display arp source-suppression コマンドを使用して、現在の ARP 送信元抑制の設定情報を表示します。

例

#現在の ARP ソース抑制の設定情報を表示します。

<Sysname> display arp source-suppression
ARP source suppression is enabled
Current suppression limit:100

表 11-1 display arp source-suppression コマンドの表示情報の説明

フィールド	説明
ARP source suppression is enabled	ARPソース抑制機能がオンになっています
Current suppression limit	5秒間隔でデバイスが受信できる送信元IPは同じですが、宛先IPアドレスが解決できないIPメッセージの最大数

11.2　ARPメッセージ速度制限設定コマンド

11.2.1 arp rate-limit

Syntax

arp rate-limit [*pps*]

undo arp rate-limit

デフォルト

ARP メッセージ速度制限がオンになっています。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

pps:ARP スロットルレート。パケット/秒(pps)で、値の範囲は 1~102400 です。このパラメータを指定しない場合は、デバイスのデフォルト ARP スロットルレートを復元するために使用されます。

説明

arp rate-limit コマンドを使用して、ARP メッセージの速度制限を有効にし、ARP メッセージの速度制限を設定します。

undo arp rate-limit コマンドは ARP メッセージ速度制限機能をオフにするために使用されます。

スロットルレートを指定しない場合、デバイスはデフォルトのスロットルレートを使用し、スロットルを超過したメッセージはドロップされます。

例

#レイヤ 2 イーサネットインタフェース GigabitEthernet1/0/1 で ARP メッセージ速度制限を有効にし、ARP メッセージ速度制限を 50 pps に設定します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp rate-limit 50

11.2.2 arp rate-limit log enable

Syntax

arp rate-limit log enable

undo arp rate-limit log enable

デフォルト

デバイスの ARP メッセージ速度制限ログ機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

arp rate-limit log enable コマンドを使用して、ARP メッセージのスロットルログ機能を有効にします。

undo arp rate-limit log enable コマンドを使用すると、ARP メッセージのスロットルログ機能が無効になります。

ARP ログ機能を有効にすると、デバイスはこの時間間隔内の速度違反のピーク値をログのレート値としてデバイスのハブに送信し、ハブのパラメータを設定することで、最終的にログメッセージの出力ルール(出力が許可されているかどうかと出力方向)を決定する。情報センターパラメータの設定については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*”の”*5 章 Information Center*”を参照してください。

例

#ARP メッセージのスロットルログ機能を有効にします。

<Sysname> system-view
[Sysname] arp rate-limit log enable

11.2.3 arp rate-limit log interval

Syntax

arp rate-limit log interval *interval*

undo arp rate-limit log interval

デフォルト

デバイスが受信する ARP メッセージレートがユーザが設定したスロットル値を超えると、デバイスがアラームとログを送信する間隔は 60 秒になります。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval:ポートの ARP メッセージレートがユーザが設定したスロットル値を超えたときに、デバイスがアラームとログを送信する間隔。値の範囲は 1~86400 で、単位は秒です。

説明

arp rate-limit log interval コマンドを使用して、デバイスが ARP メッセージレートを受信したときに、デバイスがアラームとログを送信する間隔を設定します。

undo arp rate-limit log interval コマンドを使用して、デフォルトの状態を復元します。

ユーザはアラームまたはログを送信する機能をオンにしてから、デバイスがアラームおよびログを送信する間隔を指定するようにこのコマンドを設定する必要があります。また、このコマンドはポートで **arp rate-limit** コマンドと一緒に使用する必要があります。このコマンドを個別に設定しても効果はありません。

例

#デバイスが受信する ARP メッセージのレートがユーザが設定したスロットル値を超える場合、デバイスがアラームとログを送信する間隔を 120 秒に設定します。

<Sysname> system-view
[Sysname] arp rate-limit log interval 120

関連コマンド

- **arp rate-limit**
- **arp rate-limit log enable**
- **snmp-agent trap enable arp**

11.2.4 snmp-agent trap enable arp

Syntax

snmp-agent trap enable arp [**rate-limit**]

undo snmp-agent trap enable arp [**rate-limit**]

デフォルト

ARP モジュールのアラーム機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

rate-limit:ARP メッセージ速度制限のアラーム機能をオンにします。

説明

snmp-agent trap enable arp コマンドを使用して、ARP モジュールのアラーム機能をオンにします。

undo snmp-agent trap enable arp コマンドを使用して、ARP モジュールのアラーム機能をオフにします。

ARP モジュールの警報機能を起動した後、設備はこの時間間隔内の速度超過ピーク値を警報情報として発送する、生成した警報情報は設備の SNMP モジュールに発送する、SNMP 中の警報情報の発送パラメータを設置することによって、警報情報出力の相関特性を決定する。

アラーム情報の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*17 ネットワーク管理と監視*”の” *4 章 SNMP*”を参照してください。

例

#ARP メッセージ速度制限のアラーム機能を有効にします。

<Sysname> system-view
[Sysname] snmp-agent trap enable arp rate-limit

11.3　送信元MACアドレス固定ARPアタック検出設定コマンド

11.3.1 arp source-mac

Syntax

arp source-mac { **filter** | **monitor** }

undo arp source-mac [**filter** | **monitor**]

デフォルト

送信元 MAC アドレスが固定されている ARP アタック検出機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

filter:フィルタモードでチェックモードを設定します。

monitor:モニタモードでチェックモードを設定します。

説明

arp source-mac コマンドを使用して、送信元 MAC アドレスが固定された ARP アタック検出機能を有効にし、検査モードを選択します。

undo arp source-mac コマンドは、送信元 MAC アドレスが固定されている ARP アタック検出機能を無効にするために使用します。

ゲートウェイデバイスでこの機能をオンにすることをお勧めします。

本機能は、 ARP パケットの送信元 MAC アドレスから CPU に送信された ARP パケットをカウントし、 5 秒間に同一の送信元 MAC アドレス(ソース MAC アドレス固定)を宛先とする ARP パケットが一定のしきい値を超えた場合に攻撃があったと見なし、システムがその MAC アドレスを攻撃検知エントリに追加する。ARP ログ情報機能(**arp check log enable** コマンドの設定)が有効になっていて、攻撃検出テーブルのエントリが古くなる前に、設定された検査モードがフィルタモードである場合、ログ情報が印刷され、送信元 MAC アドレスから送信された ARP メッセージがフィルタリングされます。監視モードに設定すると、ログ情報のみが出力され、送信元 MAC アドレスから送信された ARP メッセージはフィルタリングされません。ARP ログ情報機能の詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*5 ネットワーク接続*”の”*8 章 ARP*”を参照してください。

検査モードが **undo arp source-mac** コマンドで指定されていない場合は、任意の検査モードの送信元 MAC アドレス固定 ARP アタック検出機能を無効にします。

例

#送信元 MAC アドレス固定 ARP アタック検出機能をオンにし、filter チェックモードを選択します。

<Sysname> system-view
[Sysname] arp source-mac filter

11.3.2 arp source-mac aging-time

Syntax

arp source-mac aging-time *time*

undo arp source-mac aging-time

デフォルト

送信元 MAC アドレス固定 ARP アタック検出テーブルエントリのエージングタイムは 300 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

time:送信元 MAC アドレスが固定の ARP アタック検知エントリのエージングタイムは、60ら6000 の範囲の値をとり、単位は秒である。

説明

arp source-mac aging-time コマンドを使用して、送信元 MAC アドレスの固定 ARP アタック検出テーブルエントリのエージングタイムを設定します。

undo arp source-mac aging-time コマンドを使用して、デフォルトの状態を復元します。

例

#設定ソース MAC アドレス固定 ARP アタック検出テーブルエントリのエージングタイムは 60 秒です。

<Sysname> system-view
[Sysname] arp source-mac aging-time 60

11.3.3 arp source-mac exclude-mac

Syntax

arp source-mac exclude-mac *mac-address*&<1-n>

undo arp source-mac exclude-mac [*mac-address*&<1-n>]

デフォルト

保護 MAC アドレスが設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address& *<1-n>*:MAC アドレスのリスト。ここで、mac-address は、H-H-H の形式で設定された保護された MAC アドレスです。&<1-n>は、一度に設定できる保護 MAC アドレスの最大数です。n の値は 10 です。

説明

保護された MAC アドレスを設定するには、**arp source-mac exclude-mac** コマンドを使用します。保護された MAC アドレスが設定されている場合、ARP メッセージ内の MAC アドレスに攻撃があっても、フィルタリングは検出されません。

undo arp source-mac exclude-mac コマンドは、設定されている保護された MAC アドレスを削除します。

undo コマンドで MAC アドレスが指定されていない場合は、設定されている保護された MAC アドレスをすべて削除します。

例

#設定ソース MAC アドレス固定 ARP アタックは 001 e-1200-0213 の保護 MAC アドレスをチェックします。

<Sysname> system-view
[Sysname] arp source-mac exclude-mac 001e-1200-0213

11.3.4 arp source-mac threshold

Syntax

arp source-mac threshold *threshold-value*

undo arp source-mac threshold

デフォルト

送信元 MAC アドレス固定 ARP パケット攻撃検出しきい値は 30 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

threshold-value:一定時間内でのソース MAC アドレス固定の ARP パケット攻撃検知の閾値、単位はパケット数、範囲は 1~5000 である。

説明

arp source-mac threshold コマンドを使用して、送信元 MAC アドレスが固定された ARP メッセージを一定時間(5 秒)受信した場合に ARP メッセージ攻撃があると見なす、ARP 固定メッセージ攻撃検出しきい値を設定します。

undo arp source-mac threshold コマンドを使用して、デフォルトの状態を復元します。

例

#設定ソース MAC アドレス固定 ARP パケット攻撃検出しきい値は 30 です。

<Sysname> system-view
[Sysname] arp source-mac threshold 30

11.3.5 display arp source-mac

Syntax

display arp source-mac [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface interface-type interface-number:指定されたインタフェースで検出された送信元 MAC アドレス固定 ARP アタック検出テーブルエントリを表示します。interface-type interface-number は、指定されたインタフェースのタイプと数を示します。

説明

display arp source-mac コマンドを使用して、検出された送信元 MAC アドレスの固定 ARP アタック検出テーブルエントリを表示します。

例

#インタフェース GigabitEthernet1/0/1 で検出された送信元 MAC アドレス固定 ARP アタック検出テーブルエントリを表示します。

<Sysname> display arp source-mac interface gigabitethernet 1/0/1

Source-MACVLAN IDInterfaceAging-time

23 f3-1122-33444094GE1/0/110

表 11-2 display arp source-mac コマンドの表示情報の説明

フィールド	説明
Source-MAC	攻撃が検出された送信元MACアドレス
VLAN ID	攻撃が検出されたVLAN ID
Interface	攻撃元のインタフェース
Aging-time	ARP Anti-Attack Policyテーブルエントリのエージングタイムの残り時間を分単位で指定します。

11.4 ARPメッセージ送信元MACアドレスの整合性チェック設定コマンド

11.4.1 arp valid-check enable

Syntax

arp valid-check enable

undo arp valid-check enable

デフォルト

ARP メッセージの送信元 MAC アドレスの整合性チェック機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

説明

arp valid-check enable コマンドを使用して、ARP メッセージの送信元 MAC アドレスの整合性チェック機能を有効にします。

undo arp valid-check enable コマンドは、ARP メッセージの送信元 MAC アドレスの整合性チェック機能を無効にするために使用します。

ARP メッセージの送信元 MAC アドレスの整合性チェック機能は、主にゲートウェイデバイスに適用されます。

ARP メッセージの送信元 MAC アドレスの整合性チェックを有効にすると、デバイスは受信した ARP メッセージをチェックし、イーサネットデータフレームの先頭の送信元 MAC アドレスと ARP メッセージの送信元 MAC アドレスが異なる場合は、そのメッセージを破棄します。

例

#ARP メッセージの送信元 MAC アドレスの整合性チェック機能を有効にします。

<Sysname> system-view
[Sysname] arp valid-check enable

11.5 ARPプロアクティブ確認設定コマンド

11.5.1 arp active-ack enable

Syntax

arp active-ack [**strict**] **enable**

undo arp active-ack [**strict**] **enable**

デフォルト

ARP プロアクティブ確認機能がオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

strict:ARP プロアクティブ確認機能の strict モード。

説明

arp active-ack enable コマンドを使用して、ARP プロアクティブ認証を有効にします。

undo arp active-ack enable コマンドを使用して、ARP プロアクティブ確認機能を無効にします。

ARP のプロアクティブな確認機能は、主にゲートウェイデバイスに適用され、攻撃者がユーザになりすましてゲートウェイデバイスをだますのを防ぎます。

例

#ARP プロアクティブ確認を有効にします。

<Sysname> system-view
[Sysname] arp active-ack enable

11.6 ARPアタック検知設定コマンド

11.6.1 arp detection enable

Syntax

arp detection enable

undo arp detection enable

デフォルト

ARP アタック検知機能がオフになっているため、ユーザの正当性チェックは行われません。

View

VLAN view

定義済みユーザロール

network-admin

説明

arp detection enable コマンドは、ARP メッセージのユーザ正当性チェックとして ARP アタック検知機能を有効にするために使用します。

undo arp detection enable コマンドは、ARP アタック検知機能をオフにするために使用します。

例

#VLAN 2 で ARP Detection を有効にします。

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable

関連コマンド

- **arp detection rule**
- **display arp detection**

11.6.2 arp detection trust

Syntax

arp detection trust

undo arp detection trust

デフォルト

インタフェースは ARP 非信頼インタフェースで、AC は ARP 非信頼 AC です。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

arp detection trust コマンドを使用して、インタフェースを ARP 信頼インタフェースに設定するか、AC を ARP 信頼 AC に設定します。

undo arp detection trust コマンドを使用して、デフォルトの状態を復元します。

例

#レイヤ 2 イーサネットインタフェース GigabitEthernet1/0/1 を ARP 信頼インタフェースに設定します。

<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust

11.6.3 arp detection validate

Syntax

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

デフォルト

ARP メッセージの有効性チェックがオフになっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

dst-mac:ARP応答メッセージ中の宛先MACアドレスが､全0または全1であり、Ethernetヘッダ中の宛先 MAC アドレスと一致しているかどうかを調べる。全 0,全 1,不一致のメッセージはすべて無効であり、無効なメッセージは破棄する必要がある。

ARP メッセージの送信元 IP アドレスと宛先 IP アドレス、すべて 1、またはマルチキャスト IP アドレスが無効であることを確認し、ドロップする必要があります。ARP 応答メッセージでは、送信元 IP アドレスと宛先 IP アドレスの両方がチェックされます。ARP 要求メッセージの場合は、送信元 IP アドレスのみがチェックされます。

src-mac:ARP メッセージの送信元 MAC アドレスと Ethernet ヘッダの送信元 MAC アドレスが一致しているかどうかを確認し､一致している場合は有効､一致していない場合は破棄します。

説明

arp detection validate コマンドを使用して、ARP メッセージの宛先 MAC アドレスまたは送信元 MAC アドレスと IP アドレスの妥当性チェックをオンにします。

undo arp detection validate コマンドを使用して、ARP メッセージの妥当性検査を無効にします。

有効性チェックをオンにすると､1 つのチェックを指定したり､複数のチェックを組み合わせて構成したりできます。

「閉じる」 では、1 つ以上のチェックを閉じるように指定できます。チェック方法を指定しない場合は、すべての妥当性チェックが閉じられます。

例

#ARP メッセージの MAC アドレスと IP アドレスの有効性チェックをオンにします。

<Sysname> system-view
[Sysname] arp detection validate dst-mac ip src-mac

11.6.4 arp restricted-forwarding enable

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

デフォルト

ARP メッセージ強制転送機能がオフになっています。

View

VLAN view

定義済みユーザロール

network-admin

説明

arp restricted-forwarding enable コマンドを使用して、ARP メッセージの強制転送を有効にします。

undo arp restricted-forwarding enable コマンドは、ARP メッセージ強制転送機能を無効にするために使用します。

例

#VLAN 2 の ARP メッセージ強制転送機能を有効にします。

<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp restricted-forwarding enable

11.6.5 display arp detection

Syntax

display arp detection

View

すべての view

定義済みユーザロール

network-admin

network-operator

View

display arp detection コマンドは、ARP アタック検知機能が設定された VLAN を表示するために使用されます。

例

#ARP アタック検知機能が設定されているすべての VLAN を表示します。

<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1-2, 4-5

表 11-3　display arp detection コマンドの表示情報の説明

フィールド	説明
ARP detection is enabled in the following VLANs	ARPアタック検知機能が設定されているVLAN情報、またはARPアタック検知機能が設定されているVLANが存在しない場合は「ARP detection is not enabled in any VLANs.」

関連コマンド

- **arp detection enable**

11.6.6 display arp detection statistics attack-source

Syntax

display arp detection statistics attack-source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

ARP アタック元の統計情報を表示するには、**display arp detection statistics attack-source** コマンドを使用します。このコマンドは、ARP アタック元の最大 1023 の統計エントリと 1 つの識別エントリを表示します。

初めて最大数に達すると、デバイスは最も古い統計エントリを最新の統計エントリで上書きし、識別エントリを生成します。識別エントリのパラメータは次のとおりです。

- インタフェース、VLAN、MAC アドレス、および IP アドレスの各フィールドは空です。
- Number フィールドには、上書きされた古いエントリに格納されている Number の値が表示されます。
- Time フィールドには、識別エントリが生成された時刻が表示されます。

その後、新しい統計エントリが生成されるたびに、デバイスは次のように識別エントリを更新します。

- 新しいエントリの Number フィールド値を Number フィールドの現在の値に加算します。
- Time フィールド値をこの識別エントリが更新された時刻に置き換えます。

例

#スロット 1 の ARP アタック元の統計情報を表示します。

<Sysname> display arp detection statistics attack-source slot 1

```
Interface            VLAN  MAC address    IP address      Number     Time
GE1/0/1              1     0005-0001-0001 10.1.1.14       24         17:09:56
03-27-2017
```

表 11-4 display arp detection statistics コマンドの表示情報の説明

フィールド	説明
Interface	ARPアタックパケットの受信インタフェース。
VLAN	ARPアタックパケットが属するVLAN。
MAC address	ARPアタックパケットの送信元MACアドレス。
IP address	ARPアタックパケットの送信元IPアドレス。
Number	ARPアタック検出によってドロップされたARPアタックパケットの数。
Time	ARPアタック検出によってARPアタックパケットがドロップされた最新の時刻。

関連コマンド

- **reset arp detection statistics attack-source**

11.6.7 display arp detection statistics packet-drop

Syntax

display arp detection statistics packet-drop [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*:指定したインタフェースの ARP Detection ドロップメッセージの統計情報を表示します。interface-type interface-number インタフェースのタイプと番号を指定するために使用します。このパラメータを指定しない場合、すべてのインタフェースの ARP Detection ドロップメッセージの統計情報が表示されます。

説明

ARP アタック検出によってドロップされたパケットの統計情報を表示するには、**display arp detection statistics packet-drop** コマンドを使用します。

例

#ARP Detection ドロップメッセージの統計を表示します。

<Sysname> display arp detection statistics packet-drop

```
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)          IP       Src-MAC   Dst-MAC   Inspect
GE1/0/1(U)               40       0         0         78
GE1/0/2(U)               0        0         0         0
GE1/0/3(T)               0        0         0         0
GE1/0/4(U)               0        0         30        0
```

表 11-5 display arp detection statistics コマンドの表示情報の説明

フィールド	説明
State	インタフェースの状態: • U:ARP非信頼インタフェース • T:ARP信頼インタフェース
Interface (State)	ARPメッセージがインタフェースに着信します。 Stateは、インタフェースの信頼状態を示します。

フィールド	説明
IP	ARPメッセージの送信元IPアドレスと宛先IPアドレスのチェックが、ドロップされたメッセージ数に失敗しました
Src-MAC	ARPメッセージの送信元MACアドレスのチェックで、ドロップされたメッセージ数に失敗しました
Dst-MAC	ARPメッセージの宛先MACアドレスのチェックが、ドロップされたメッセージ数に失敗しました
Inspect	ARPメッセージはユーザの正当性チェックと結合され、ドロップされたメッセージ数を通過しません。

関連コマンド

- reset arp detection statistics packet-drop

11.6.8 reset arp detection statistics attack-source

Syntax

reset arp detection statistics attack-source

View

User view

定義済みユーザロール

network-admin

説明

ARP アタック元の統計情報をクリアするには、**reset arp detection statistics attack-source** コマンドを使用します。

例

#すべての ARP アタック元の統計情報をクリアします。

<Sysname> reset arp detection statistics attack-source

関連コマンド

- **display arp detection statistics attack-source**

11.6.9 reset arp detection statistics packet-drop

Syntax

reset arp detection statistics packet-drop [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースの下の ARP Detection のメッセージドロップ統計情報をクリアすることを示します。interface-type interface-number インタフェースのタイプと番号を指定するために使用します。このパラメータが指定されていない場合は、すべてのインタフェースの ARP Detection メッセージドロップ統計情報がクリアされます。

説明

reset arp detection statistics コマンドは、ARP Detection のメッセージドロップ統計情報をクリアするために使用されます。

例

#すべての ARP Detection のためのメッセージドロップ統計情報をクリアします。

<Sysname> reset arp detection statistics packet-drop

関連コマンド

- display arp detection statistics packet-drop

11.7 ARP自動スキャン、プロファイリング設定コマンド

11.7.1 arp scan

Syntax

arp scan [*start-ip-address* **to** *end-ip-address*]

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

start-ip-address:ARP スキャンインターバルの開始 IP アドレス。開始 IP アドレスは、終了 IP アドレス以下である必要があります。

end-ip-address:ARP スキャン区間の終端 IP アドレス。

説明

arp scan コマンドを使用して、ARP 自動スキャン機能を有効にします。

 注意

スキャンには時間がかかる場合があり、デバイスリソースとネットワーク負荷が大きくなります。スキャンを終了するには、<Ctrl_C> (スキャンを終了すると、受信したネイバー応答に対して、そのネイバーのダイナミック ARP テーブルエントリが確立されます。) を使用します。

ARP 自動スキャン機能は、インタフェースで指定されたアドレス範囲内のネイバーをスキャンし、すでに ARP テーブルエントリが存在する IP アドレスはスキャンしません。

ユーザがローカルエリアネットワーク内のネイバーに割り当てられた IP アドレスの範囲を知っており、ARP スキャン区間を指定した場合、その範囲内のネイバーがスキャンされ、スキャン待ち時間が短縮される。指定されたスキャンゾーンがインタフェースの複数の IP アドレスのネットワークセグメントに同時に存在する場合、送信される ARP 要求メッセージの送信元 IP アドレスは、ネットワークセグメントの範囲が狭いインタフェース IP アドレスを選択します。

ユーザが ARP スキャンインターバルの開始 IP アドレスと終了 IP アドレスを指定しない場合、インタフェースのプライマリ IP アドレスセグメント内のネイバーのみがスキャンされます。ここで、送信される ARP 要求メッセージの送信元 IP アドレスは、インタフェースのプライマリ IP アドレスです。

ARP スキャンインターバルの開始 IP アドレスと終了 IP アドレスは、インタフェースの IP アドレス(マスターIP アドレスまたは手動で設定したスレーブ IP アドレス)と同じネットワークセグメントにある必要があります。

例

#インタフェース Vlan-interface2 のプライマリ IP アドレスネットワークセグメント内のネイバーをスキャンします。

<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan

#インタフェース Vlan-interface2 で指定されたアドレス範囲内のネイバーをスキャンします。

<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

16. QoS

本マニュアルは以下に示す章で構成されています。

01- QoS ポリシー
02- プライオリティマッピング
03- WLAN QoS

目次

このセクションのページは **16-x-x** です。

1 章 QoS ポリシー 1-1
1.1 トラフィッククラス設定コマンド 1-1
1.1.1 description 1-1
1.1.2 display traffic classifier 1-1
1.1.3 if-match 1-3
1.1.4 traffic classfier 1-7
1.2 トラフィック動作設定コマンド 1-8
1.2.1 car 1-8
1.2.2 display traffic behavior 1-9
1.2.3 filter 1-10
1.2.4 remark dscp 1-11
1.2.5 remark local-precedence 1-12
1.2.6 traffic behavior 1-13
1.3 QoS ポリシー設定コマンド 1-14
1.3.1 classifier behavior 1-14
1.3.2 display qos policy 1-15
1.3.3 display qos policy interface 1-16
1.3.4 qos apply policy (interface view) 1-19
1.3.5 qos policy 1-20

1章 QoS ポリシー

1.1 トラフィッククラス設定コマンド

1.1.1 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Traffic class view

定義済みユーザーロール

network-admin

パラメータ

text：説明を指定します。設定範囲は 1~127 文字です。大文字と小文字を区別します。

説明

description コマンドは、クラスの説明を設定します。

undo description コマンドは、デフォルトに戻します。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

#トラフィッククラス class1 の classifier として説明を設定します。

<Sysname> system-view

[Sysname] traffic classifier class1

[Sysname-classifier-class1] description classifier

1.1.2 display traffic classifier

Syntax

display traffic classifier user-defined [*classifier-name*]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

user-difined:ユーザー定義のトラフィッククラスを指定します。

classifier-name: トラフィッククラスを指定します。設定範囲は 1~31 文字です。指定しない場合、すべてのトラフィッククラスを表示します。

説明

display traffic classifier コマンドはトラフィッククラスを表示します。

例

#ユーザー定義のすべてのトラフィッククラスを表示します。

<Sysname> display traffic classifier user-defined

```
User-defined classifier information:

Classifier:1 (ID 100)
Operator:AND
Rule (s) :
If-match acl 2000

Classifier:2 (ID 101)
Operator:AND
Rule (s) :
If-match protocol ipv6

Classifier:3 (ID 102)
Operator:AND
Rule (s) :
-none-
```

表 1-1 コマンド出力

フィールド	説明
Classifier	クラスの名前とその内容。内容には複数のタイプがあります。
Operator	分類規則間の論理関係
Rule (s)	分類規則

1.1.3 if-match

Syntax

if-match [**not**] *match-criteria*

undo if-match [**not**] *match-criteria*

デフォルト

設定なし

View

Traffic class view

定義済みユーザーロール

network-admin

パラメータ

not: 一致しません。

*match-criteria:*一致条件を指定します。表 1-2 に使用可能な一致条件を示します。

表 1-2 使用可能な一致条件

フィールド	説明
acl [ipv6 |mac] {*acl-number* |**name** *acl-name* **}**	ACLでマッチするように指定します。 *acl-number*はACLの番号でACLを指定します。 ● IPv4 ACLの設定範囲は2000~3999です。 ● IPv6 ACLの設定範囲は2000~3999です。 ● レイヤ2ACLの設定範囲は4000~4999です。 *acl-na*me は ACL 名で ACL を指定します。設定範囲は 1~63 文字です。大文字と小文字を区別しません。文字列の最初は英字を指定します。混同を避けるため、パラメータがすべてではないことを確認してください。
any	すべてのパケットに一致するように指定します。
customer-dot1p *dot1p-value*& <*1-8*>	2重にタグが付いたパケットの内部VLANタグの802.1pプライ オリティにマッチするように指定します。dot1p -value &<1-8>は、設定範囲が0～7の802.1pプライオリティ値のリストです。&<1-8>を使用して最大8つの802.1pプライオリティ値を指定できます。
customer-vlan-id *vlan-id-list*	2重タグ付きパケットの内部VLANタグ内のVLAN IDと一致します。 vlan-id-list引数には、最大10個のVLAN項目をスペースで区切ったリストを指定します。各項目は、VLANまたはVLANの範囲をvlan-id 1~vlan-id 2の形式で指定します。vlan-id 2の値は、vlan-id 1の値以上である必要があります。vlan-id引数の値の範囲は1から4094です。
destination-mac *mac-address*	指定した宛先MACアドレスのパケットにマッチするよう指定します。 このオプションは、Ethernetインタフェースでのみ有効です。
dscp *dscp-value*& <*1-8*>	DSCP値あるいはキーワードでマッチするように指定します。dscp-valueは、設定範囲が0～63のDSCP値のリストです。&<1-8>を使用して最大8つまでDSCP値を設定できます。 dscp-valueのキーワードを表 1-4に示します。
ip-precedence *ip-precedence-value*& <1-8>	パケットのIPプレシーデンスにマッチするよう指定します。ip-precedence-valueは、設定範囲が0～7のIPプレシーデンス値 のリストです。&<1-8>を使用して最大8つのIPプレシーデンス値を指定できます。

フィールド	説明
local-precedence local-*precedence-value*& <*1-8*>	ローカルプレシーデンスにマッチするよう指定します。precedence-valueは、設定範囲が0～7のIPプレシーデンス値のリストです。&<1-8>を使用して最大8つのローカルプレシーデンス値を指定できます。
protocol *protocol-name*	指定したプロトコルのパケットにマッチするように指定します。protocol-nameはIP、IPv6が指定できます。
source-mac *mac-address*	指定した送信元MACアドレスのパケットにマッチするよう 指定します。このオプションは、Ethernetインタフェースでのみ有効です。

説明

if-match コマンドは一致条件を定義します。

undo if-match コマンドは一致条件を削除します。

1 つのクラスで複数のマッチするコマンドを設定でき、各設定が重複することはありません。

一致条件のコントロールプレーン、DSCP、IP 優先順位、ローカルプレシーデンスを指定するときは、次の点に注意してください。

- コマンドには複数の一致条件を設定することができます。同じ設定が複数ある場合、システムはデフォルトで 1 つとみなします。異なる一致条件はOR関係にあります。
- 一致条件を削除する場合は、定義されている順序と同じでなければ削除できません。

ACL に一致条件を指定する場合、クラスで参照される ACL はすでに存在している必要があります。

if-match で参照されている ACL のアクションを deny にすることはできません。deny を使用すると、一致条件が設定されていない場合と同じになり、マッチが無効になります。

マッチするクラスの一致条件を指定するときに、マッチするクラスの一致条件間に AND と OR の両方が含まれる場合は、次のように設定します。たとえば、一致条件 1&一致条件 2|一致条件 3 の関係を満たす classA を以下のように指定します。

- traffic classifier classB operator and
  - if-match 一致条件 1
  - if-match 一致条件 2
- traffic classifier classA operator or
  - if-match 一致条件 3
  - if-match classifier classB

例

#宛先 MAC アドレスが 0050-ba27-bed3 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class1

[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3

#送信元 MAC アドレスが 0050-ba27-bed2 のパケットのマッチングを行うように、トラフィッククラス class2 に一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class2

[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2

VLAN タグの 802.1p プライオリティ 3 のパケットとマッチングを行うように、トラフィッククラス class1 の一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class1

[Sysname-classifier-class1] if-match customer-dot1p 3

拡張 ACL 3101 のマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class1

[Sysname-classifier-class1] if-match acl 3101

#ACL IPv6 ACL3101 のマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class1

[Sysname-classifier-class1] if-match acl ipv6 3101

#すべてのパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class1

[Sysname-classifier-class1] if-match any

DSCP が 1、6、9 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class1 operator or

[Sysname-classifier-class1] if-match dscp 1 6 9

IP プレシーデンスが 1、6 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class1 operator or

[Sysname-classifier-class1] if-match ip-precedence 1 6

ローカルプレシーデンスが 1、6 のパケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class1 operator or

[Sysname-classifier-class1] if-match local-precedence 1 6

IP パケットのマッチングを行うように、トラフィッククラス class1 に一致条件を定義します。

<Sysname> system-view

[Sysname] traffic classifier class1

[Sysname-classifier-class1] if-match protocol ip

1.1.4 traffic classfier

Syntax

traffic classifier *classfier-name*[**operator**{**and**|**or**}]

undo traffic classifier *classifier-name*

デフォルト

設定なし

View

System view

定義済みユーザーロール

network-admin

パラメータ

classifier-name: トラフィッククラスを指定します。大文字と小文字を区別します。設定範囲は 1～31 文字です。

operator: トラフィッククラスの論理積 AND あるいは論理和 OR を指定するオペレータを設定します。デフォルトは論理積 AND です。

and: 論理積 AND を指定します。トラフィッククラスはすべての条件に一致したパケットのみマッチングします。

or: 論理和 OR を指定します。トラフィッククラスはいずれかの条件に一致したパケットのみマッチングします。

説明

traffic classifier コマンドはトラフィッククラスを作成し、traffic class view に移行します。

undo traffic classifier コマンドはトラフィッククラスを削除します。

例

トラフィッククラス class1 を作成します。

<AC> system-view

[AC] traffic classifier class1

[AC-classifier-class1]

関連コマンド

display traffic classifier

1.2 トラフィック動作設定コマンド

1.2.1 car

Syntax

car cir *committed-information-rate* [**cbs** *committed-burst-size*] [**green** *action* |**red** *action*]*

undo car

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザーロール

network-admin

パラメータ

cir *committed-information-rate*: CIR（認定情報レート）を kbps 単位で指定します。設定範囲は 8～10000000 です。

cbs *committed-burst-size*: CBS（認定バーストサイズ）を byte 単位で指定します。設定範囲は 1000～1000000000 です。

green *action*: CIR に対応するパケットに対して実施されるアクションを指定します。デフォルトはパケットを転送します。

red *action*: CIR に対応しないパケットに対して実施されるアクションを指定します。デフォルトはパケットを廃棄します。

action: パケットに対して実施されるアクションを指定します。

- **discard**: パケットを廃棄します。
- **pass**: パケットを転送します。

説明

car コマンドはトラフィック動作に CAR アクションを設定します。

undo car コマンドはトラフィック動作から CAR アクションを削除します。

同一のトラフィック動作に car コマンドを複数設定した場合、最後に行った設定が適用されます。

例

トラフィック動作に CAR アクションを設定します。

<AC> system-view

[AC] traffic behavior database

[AC-behavior-database] car cir 200 cbs 51200 green pass

1.2.2 display traffic behavior

Syntax

display traffic behavior user-defined[*behavior-name*]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

user-defined: ユーザー定義のトラフィック動作を表示します。

behavior-name: トラフィック動作を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのトラフィック動作を表示します。

説明

display traffic behavior コマンドは、トラフィック動作を表示します。

例

#すべてのユーザー定義のトラフィック動作を表示します。

<Sysname> display traffic behavior user-defined

```
User-defined behavior information:

Behavior:1 (ID 100)
Committed Access Rate:
CIR 112 (kbps)、CBS 5120 (Bytes)
Green action:pass
Red action:discard
```

表 1-3 コマンド出力

フィールド	説明
User-defined behavior information	ユーザー定義のフロー動作に関する情報
Behavior	トラフィック動作の名前と内容
Committed Access Rate	CARアクションの情報です。
CIR	認定情報レート、kbps
CBS	バイト単位のバーストサイズを約束
Green action	greenパケットを適用するアクションです。
Red action	redパケットを適用するアクションです。

1.2.3 filter

Syntax

filter {**deny** |**permit** }

undo filter

デフォルト

設定なし

View

traffic behavior view

定義済みユーザーロール

network-admin

パラメータ

deny: パケットを廃棄します。

permit: パケットを転送します。

説明

filter コマンドはトラフィック動作にトラフィックフィルタリングを設定します。

undo filter コマンドはトラフィック動作からトラフィックフィルタリングを削除します。

例

トラフィック動作 database にパケットを廃棄するトラフィックフィルタリングを設定します。

<AC> system-view

[AC] traffic behavior database

[AC-behavior-database] filter deny

1.2.4 remark dscp

Syntax

remark dscp *dscp-value*

undo remark dscp

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザーロール

network-admin

パラメータ

dscp-value: DSCP 値あるいは DSCP のキーワードを指定します。DSCP 値の設定範囲は 0～63 です。DSCP のキーワードを表 1-4 に示します。

表 1-4 DSCP のキーワードと値

キーワード	DSCP 値(バイナリ)	DSCP 値(10 進法)
af 11	001010	10
af 12	001100	12
af 13	001110	14
af 21	010010	18
af 22	010100	20
af 23	010110	22
af 31	011010	26
af 32	011100	28

キーワード	DSCP 値(バイナリ)	DSCP 値(10 進法)
af 33	011110	30
af 41	100010	34
af 42	100100	36
af 43	100110	38
cs 1	001000	8
cs 2	010000	16
cs 3	011000	24
cs 4	100000	32
cs 5	101000	40
cs 6	110000	48
cs 7	111000	56
default	000000	0
ef	101110	46

説明

remark dscp コマンドはトラフィック動作に DSCP マーキングアクションを設定します。

undo remark dscp コマンドは DSCP マーキングアクションを削除します。

例

トラフィックの DSCP 値を 6 に設定します。

<Sysname> system-view

[Sysname] traffic behavior database

[Sysname-behavior-database] remark dscp 6

1.2.5 remark local-precedence

Syntax

remark local-precedence *local-precedence-value*

undo remark local-precedence

デフォルト

設定なし

View

Traffic behavior view

定義済みユーザーロール

network-admin

パラメータ

local-precedence-value: パケットに設定するローカルプレシーデンスを指定します。設定範囲は 0～7 です。

説明

remark local-precedence コマンドはトラフィック動作にローカルプレシーデンスアクションを設定します。

undo remark local-precedence コマンドはアクションを削除します。

例

トラフィック動作にローカルプレシーデンスを 2 にするアクションを設定します。

<AC> system-view

[AC] traffic behavior database

[AC-behavior-database] remark local-precedence 2

1.2.6 traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic *behavior behavior-name*

デフォルト

設定なし

View

system-view

定義済みユーザーロール

network-admin

パラメータ

behavior-name:トラフィック動作を設定します。大文字と小文字を区別します。設定範囲は 1~31 です。

説明

traffic behavior コマンドはトラフィック動作を作成し、traffic behavior view に移行します。すでにトラフィック動作がある場合、その view に移行します。

undo traffic behavior コマンドはトラフィック動作を削除します。

例

トラフィック動作 behavior1 を作成します。

<AC> system-view

[AC] traffic behavior behavior1

[AC-behavior-behavior1]

関連コマンド

display traffic behavior

1.3 QoSポリシー設定コマンド

1.3.1 classifier behavior

Syntax

classifier *classifier-name* **behavior behavior-name** [**insert-before** *before-classifier-name*]

undo classifier classifier-name

デフォルト

設定なし

View

QoS policy view

定義済みユーザーロール

network-admin

パラメータ

classifier-name: トラフィッククラスを指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

behavior-name: トラフィック動作を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

insert-before *before-classifier-name*: QoS ポリシー内の既存のトラフィッククラスの前に、新規のトラフィッククラスを挿入します。*before-classifier-name* で既存のトラフィッククラスの名前を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。**insert-before** *before-classifier-name* パラメータを指定しない場合、新規のトラフィッククラスは QoS ポリシーの最後に挿入されます。

説明

classifier behavior コマンドはトラフィック動作を QoS ポリシーのトラフィッククラスに関連づけます。

undo classifier コマンドは QoS ポリシーからトラフィッククラスを削除します。

QoS ポリシーのトラフィッククラスは 1 つのトラフィック動作にのみ関連づけることができます。

指定したトラフィッククラスあるいはトラフィック動作が存在しない場合、システムは null のトラフィッククラスまたはトラフィック動作を作成します。

undo classifier default-class コマンドは以下の動作を実行します。

- システム定義のクラス default-class に対する既存のクラス動作の関連付けを削除します。
- システム定義のクラス default-class を、システム定義の動作 be に関連付けます。

例

トラフィック動作 test を QoS ポリシーuser1 のトラフィッククラス database に関連づけます。

<AC> system-view

[AC] qos policy user1

[AC-qospolicy-user1] classifier database behavior test

トラフィック動作 test を QoS ポリシーuser1 のトラフィッククラス database に関連づけ、トラフィッククラス database を既存のトラフィッククラス class-a の前に挿入します。

<AC> system-view

[AC] qos policy user1

[AC-qospolicy-user1] classifier database behavior test insert-before class-a

関連コマンド

qos policy

1.3.2 display qos policy

Syntax

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

user-defined: ユーザー定義の QoS ポリシーを表示します。

policy-name: QoS ポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのユーザー定義の QoS ポリシーを表示します。

classifier *classifier-name*: トラフィッククラス名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。指定しない場合、すべてのトラフィッククラスを表示します。

説明

display qos policy コマンドは QoS ポリシーを表示します。

例

すべてのユーザー定義の QoS ポリシーを表示します。

<Sysname> display qos policy user-defined

```
User-defined QoS policy information:

Policy:1 (ID 100)
Classifier:1 (ID 100)
Behavior:1
Committed Access Rate:
CIR 112 (kbps)、CBS 51200 (Bytes)
Green action:pass
Red action:discard
Classifier:2 (ID 101)
Behavior:2
-none-
```

表 1-5 コマンド出力

フィールド	説明
User-defined QoS policy information	ユーザー定義QoSポリシーの情報
System-defined QoS policy	システム定義のQoSポリシーに関する情報。
Policy	QoSポリシー名

その他の出力は及び表 1-3 を参照してください。

1.3.3 display qos policy interface

Syntax

display qos policy interface [*interface-type interface-number*] [**inbound** | **outbound**]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

interface-type *interface-number*: インタフェースのタイプと番号を指定します。インタフェースを指定しない場合、このコマンドは各インタフェースの QoS ポリシーの情報を表示します。

inbound: 受信トラフィックに適用された QoS ポリシーを表示します。

outbound: 送信トラフィックに適用された QoS ポリシーを表示します。

説明

display qos policy interface コマンドはインタフェースに適用された QoS ポリシーを表示します。

方向を指定しない場合、**inbound** と **outbound** の両方のトラフィックの QoS ポリシーを表示します。

例

GigabitEthernet 1/0/1 の受信方向のトラフィックに適用された QoS ポリシーを表示します。

<Sysname> display qos policy interface gigabitethernet 1/0/1 inbound

```
Interface:GigabitEthernet1/0/1
Direction:Inbound
Policy:1
Classifier:1
Operator:AND
Rule (s) :
If-match acl 2000
Behavior:1
Marking:
Remark dscp 3
Committed Access Rate:
CIR 112 (kbps)、CBS 51200 (Bytes)
Green action:pass
Yellow action :pass
Red action:discard
Green packets :0 (Packets) 0 (Bytes)
Yellow packets:0 (Packets) 0 (Bytes)
```

```
Red packets:0 (Packets) 0 (Bytes)
Classifier:3
Matched :0 (Packets) 0 (Bytes)
5-minute statistics:
Forwarded:0/0(pps/bps)
Dropped:0/0(pps/bps)
Operator:AND
Rule (s) :
-none-
Behavior:3
-none-
```

#すべてのインタフェースの QoS ポリシーの設定情報と動作を表示します。

<Sysname> display qos policy interface

```
Interface:GigabitEthernet1/0/1
Direction:Inbound
Policy:a
Classifier:a
Operator:AND
Rule (s) :
If-match any
Behavior:a
Committed Access Rate:
CIR 112 (kbps)、 CBS 51200 (Bytes)、 EBS 0 (Bytes)
Green action:pass
Yellow action :pass
Red action:discard
Green packets :0 (Packets)
Red packets:0 (Packets)

Interface:GigabitEthernet1/0/3
Direction:Inbound
Policy:b
Classifier:b
Operator:AND
Rule (s) :
If-match any
Behavior:b
Committed Access Rate:
CIR 112 (kbps)、 CBS 51200 (Bytes)、 EBS 0 (Bytes)
Green action:pass
Yellow action :pass
Red action:discard
```

```
Green packets :0 (Packets)
Red packets:0 (Packets)

Interface:GigabitEthernet1/0/3
Direction:Inbound
Policy:a
Classifier:a
Operator:AND
Rule (s) :
If-match any
Behavior:a
Committed Access Rate:
CIR 112 (kbps)、 CBS 51200 (Bytes)、 EBS 0 (Bytes)
Green action:pass
Yellow action :pass
Red action:discard
Green packets :0 (Packets)
Red packets:0 (Packets)
```

表 1-6 コマンド出力

フィールド	説明
Direction	インタフェースに適用されたQoSポリシーの方向です。
Matched	パケットに一致した数です。
5-minute statistics	過去5分間のトラッフィック量の統計です。
Forwarded	統計情報収集期間中に一致するパケットが正常に転送された平均レートです。
Dropped	統計情報収集期間中にドロップされた一致パケットの平均レートです。
Green packets	greenパケットのトラフィックの統計情報です。
Red packets	redパケットのトラフィックの統計情報です。

その他のコマンド出力は表 1-1 および表 1-3 を参照してください。

1.3.4 qos apply policy (interface view)

Syntax

qos apply policy *policy-name* {**inbound | autbound**}

undo qos apply policy *policy-name* {**inbound | autbound**}

デフォルト

設定なし

View

Interface-view

定義済みユーザーロール

network-admin

パラメータ

policy-name:ポリシー名を指定します。1~31 文字の文字列で、大文字と小文字が区別されます。

inbound:受信トラッフィックに QoS ポリシーが適用されます。

outbound:送信トラフィックに QoS ポリシーが適用されます。

説明

qos apply policy コマンドは QoS ポリシーをインタフェースに適用します。

undo qos apply policy コマンドは QoS ポリシーを削除します。

例

#QoS ポリシーUSER1 をインタフェース GigabitEthernet1/0/1 の送信トラフィックに適用します。

<Sysname> system-view

[Sysname] interface gigabitethernet 1/0/1

[Sysname-GigabitEthernet1/0/1] qos apply policy USER1 outbound

1.3.5 qos policy

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

デフォルト

設定なし

View

System-view

定義済みユーザーロール

network-admin

パラメータ

policy-name:QoS ポリシー名を指定します。1~31 文字の文字列で、大文字と小文字が区別されます。

説明

qos policy コマンドは QoS ポリシーを作成し、QoS policy view に移行するか、またはデフォルトの QoS policy view に移行します。

undo qos policy コマンドは QoS ポリシーを削除します。

オブジェクトに適用されているポリシーを削除するには、まず、オブジェクトからポリシーを削除する必要があります。

例

#QoS ポリシーUser1 を定義します。

<Sysname> system-view

[Sysname] qos policy user1

[Sysname-qospolicy-user1]

関連コマンド

- classifier behavior
- qos apply policy

目次

このセクションのページは **16-x-x** です。

2 章 プライオリティマッピング 2-1
2.1 プライオリティマッピング設定コマンド 2-1
2.1.1 display qos map-table 2-1
2.1.2 import 2-2
2.1.3 qos map-table 2-3
2.2 プライオリティトラステッドモード設定コマンド 2-4
2.2.1 display qos trust interface 2-4
2.2.2 qos trust 2-5
2.3 ポートプライオリティ設定コマンド 2-6
2.3.1 qos priority 2-6

2章 プライオリティマッピング

2.1 プライオリティマッピング設定コマンド

2.1.1 display qos map-table

Syntax

display qos map-table [**dot11e-lp** | **dot1p-dot1p** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp**]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

表 2-1 プライオリティマッピング

プライオリティマッピング	説明
dot11e-lp	802.11 eプライオリティマッピングです。
dot1p-lp	802.1p-localプライオリティマッピングです。
dscp-lp	DSCP-localプライオリティマッピングです。
lp-dot11e	Local-802.11eプライオリティマッピングです。
lp-dot1p	Local-802.1pプライオリティマッピングです。
lp-dscp	Local-DSCPプライオリティマッピングです。

説明

display qos map-table コマンドはプライオリティマッピングの設定を表示します。

プライオリティマップを指定しない場合、すべてのプライオリティマッピングの設定を表示します。

例

802.1p-local プライオリティマッピングの設定を表示します。

<Sysname> display qos map-table dot1p-lp

```
MAP-TABLE NAME:dot1p-lpTYPE:pre-define
IMPORT:EXPORT
0:2
```

```
1:0
2:1
3:3
4:4
5:5
6:6
7:7
```

表 2-2 コマンド出力

フィールド	説明
MAP-TABLE NAME	マッピング・テーブルの名前です。
TYPE	マッピング・テーブルのタイプです。
IMPORT	マッピング・テーブルの入力値です。
EXPORT	マッピング・テーブルの出力値です。

2.1.2 import

Syntax

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

デフォルト

デフォルトのプライオリティマッピングが使用されます。

View

Priority map view

定義済みユーザーロール

network-admin

パラメータ

import-value-list: 入力値のリストを指定します。

export-value: 出力値を指定します。

all: プライオリティマッピングのすべてのマッピングをデフォルトに戻します。

説明

import コマンドはプライオリティマッピングのマッピングを設定します。

undo import コマンドはプライオリティマッピングの指定した、あるいはすべてのマッピングをデフォルトに戻します。

例

802.1p-drop プライオリティマッピングを設定し、802.1p のプライオリティ 4 およびプライオリティ 5 を、ドロッププライオリティ 1 にマッピングします。

<AC> system-view

[AC] qos map-table dot1p-dp

[AC-maptbl-dot1p-dp] import 4 5 export 1

関連コマンド

- display qos map-table

2.1.3 qos map-table

Syntax

qos map-table { **dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp** }

View

System-view

定義済みユーザーロール

network-admin

パラメータ

パラメータの説明は表 2-1 を参照してください。

説明

qos map-table コマンドは指定した priority map view に移行します。

例

802.1p-local priority map view に移行します。

<AC> system-view

[AC] qos map-table dot1p-lp

[AC-maptbl-dot1p-lp]

関連コマンド

- display qos map-table
- import

2.2 プライオリティトラステッドモード設定コマンド

2.2.1 display qos trust interface

Syntax

display qos trust interface [*interface-type interface-number*]

View

すべての View

定義済みユーザーロール

network-admin

network-operator

パラメータ

interface-type interface-number: インターフェースのタイプと番号を指定します。指定しない場合、すべてのインターフェースのプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

説明

display qos trust interface コマンドはインターフェースのプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

例

#ポートプライオリティとトラステッドモード情報を表示します。

<Sysname> display qos trust interface gigabitethernet 1/0/1

```
Interface:GigabitEthernet1/0/1
Port priority trust information
Port priority:4
Port priority trust type:dscp、Override:disable
```

表 2-3 コマンド出力される情報

フィールド	説明
Interface	インターフェース名。インタフェースタイプとインターフェース番号で構成されます。
Port priority	インターフェースのポートプライオリティのセットです。
Port dscp priority	ポートのDSCPプライオリティです。

フィールド	説明
Port priority trust type	ポートプライオリティのトラステッドモード。次の値を取ります。 ● dot1p:802.1 p優先度 ● dscp:DSCP優先順位 ● none:すべての優先順位を信頼しない
Override	メッセージ自体の優先順位を上書きするかどうか

2.2.2 qos trust

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

デフォルト

インターフェースはパケットのプライオリティを信用しません。802.1p プライオリティとしてポートプライオリティを使用します。

View

Interface view

定義済みユーザーロール

network-admin

パラメータ

dot1p: プライオリティマッピングの受信パケットの 802.1p プライオリティを使用します。

dscp: プライオリティマッピングの受信パケットの DSCP を使用します。

説明

qos trust コマンドはインターフェースのプライオリティトラステッドモードを設定します。

undo qos trust コマンドはデフォルトのプライオリティのトラステッドモードに戻します。

VXLAN トンネルインターフェースで VXLAN メッセージの内部 IP ヘッダの DSCP プライオリティを信頼する場合，VXLAN トンネルがあるイーサネットインタフェースに qos trust dscp を設定する必要があります。

例

GigabitEthernet 1/0/1 のプライオリティトラステッドモードを 802.1p プライオリティに設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] qos trust dot1p

関連コマンド

- display qos trust interface

2.3 ポートプライオリティ設定コマンド

2.3.1 qos priority

Syntax

qos priority *priority-value*

undo qos priority

デフォルト

0

View

Interface view

定義済みユーザーロール

network-admin

パラメータ

priority-value: ポートプライオリティの値を指定します。設定範囲は 0～7 です。

説明

qos priority コマンドはインターフェースのポートプライオリティを変更します。

undo qos priority コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 のポートプライオリティを 2 に設定します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] qos priority 2

関連コマンド

- display qos trust interface

目次

このセクションのページは **16-x-x** です。

3 章 WLAN QoS 3-1
3.1 WLAN QoS 設定コマンド 3-1
3.1.1 bandwidth-guarantee 3-1
3.1.2 bandwidth-guarantee service-template 3-2
3.1.3 cac policy 3-3
3.1.4 client-rate-limit (radio view/AP group's radio view) 3-5
3.1.5 client-rate-limit (service template view) 3-7
3.1.6 client-rate-limit { disable | enable } 3-8
3.1.7 display wlan wmm 3-9
3.1.8 edca client (ac-be and ac-bk) 3-13
3.1.9 edca client (ac-vi and ac-vo) 3-15
3.1.10 edca radio 3-16
3.1.11 qos priority 3-18
3.1.12 qos trust 3-19
3.1.13 reset wlan wmm 3-20
3.1.14 svp map-ac 3-21
3.1.15 u-apsd enable 3-22
3.1.16 wlan client-rate-limit 3-22
3.1.17 wlan max-bandwidth 3-24
3.1.18 wmm 3-25

3章 WLAN QoS

3.1 WLAN QoS設定コマンド

3.1.1 bandwidth-guarantee

Syntax

bandwidth-guarantee { disable | enable }

undo bandwidth-guarantee

デフォルト

Radio view では、AP group view のサービステンプレート設定が使用されている場合、無線は AP group's radio の設定を使用します。サービステンプレートが手動で無線にバインドされている場合、帯域幅保証は無効になります。

AP group's radio では、帯域幅保証は無効になります。

View

Radio view

AP group's radio view

定義済みユーザーロール

network-admin

説明

帯域幅保証を有効にするには、**bandwidth-guarantee enable** を使用します。

帯域幅保証を無効にするには、**bandwidth-guarantee disable** を使用します。

デフォルトに戻すには、**undo bandwidth-guarantee** を使用します。

このコマンドは、ネットワークが輻輳しているときに、同じ無線に関連付けられているクライアントが保証帯域幅を取得できるようにします。保証帯域幅を設定するには、**bandwidth-guarantee service-template** コマンドを使用します。

Radio view の設定は、AP group's radio の設定よりも優先されます。

例

ap1 の保証帯域幅を設定します。

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1010

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] service-template 1

[Sysname-wlan-ap-ap1-radio-1] bandwidth-guarantee enable

AP グループ apgroup1 の保証帯域幅を設定します。

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1010

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1010] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1010-radio-1] bandwidth-guarantee enable

関連コマンド

- **bandwidth-guarantee service-template**

3.1.2 bandwidth-guarantee service-template

Syntax

bandwidth-guarantee service-template *service-template-name* **percent** *percent*

undo bandwidth-guarantee { all | service-template *service-template-name* **}**

デフォルト

Radio view では、AP group view のサービステンプレート設定が使用されている場合、無線は AP group's radio の設定を使用します。サービステンプレートが手動で無線にバインドされている場合、サービステンプレートの保証帯域幅の割合は設定されません。

AP group's radio では、サービステンプレートの保証帯域幅の割合は設定されません。

View

Radio view

AP group's radio view

定義済みユーザーロール

network-admin

パラメータ

service-template *service-template-name*:サービステンプレート名を指定します。1 から 63 文字の文字列で指定します。大文字と小文字は区別されません。指定したサービステンプレートが無線/無線インターフェースにバインドされていることを確認してください。

percent *percent*:総帯域に対する保証帯域の割合を指定します。*percent* 引数の値の範囲は 1 から 100 です。総帯域は無線の最大帯域を表します。保証帯域は、サービステンプレートに対応する BSS の最小帯域を表します。

all:すべてのサービステンプレートを指定します。

説明

bandwidth-guarantee service-template で、指定したサービステンプレートの帯域保証割合を設定します。

undo bandwidth-guarantee で、指定したサービステンプレートの帯域保証割合の設定を解除します。

このコマンドを有効にするには、帯域幅保証機能が有効になっていることを確認します。

同じ無線にバインドされているすべてのサービステンプレートについて、保証帯域幅の割合の合計が 100%を超えることはできません。

Radio view の設定は、AP group's radio view の設定よりも優先されます。

例

radio1 の service template 1 の保証帯域幅の割合を 30%に設定します。

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1010

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] service-template 1

[Sysname-wlan-ap-ap1-radio-1] bandwidth-guarantee service-template 1 percent 30

[Sysname-wlan-ap-ap1-radio-1] bandwidth-guarantee enable

AP group's radio の service template 1 の保証帯域幅の割合を 30%に設定します。

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1010

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1010] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1010-radio-1] bandwidth-guarantee enable

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1010-radio-1] service-template 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1010-radio-1] bandwidth-guarantee service-template 1 percent 30

関連コマンド

bandwidth-guarantee

wlan max-bandwidth

3.1.3 cac policy

Syntax

cac policy { **channelutilization** [*channelutilization-value*] | **client** [*client-number*] }

undo cac policy

デフォルト

radio view は、AP group's radio view の設定を使用します。

AP group's radio view では、クライアントベースのアドミッションポリシーが使用され、クライアントの最大数は 20 です。

View

Radio view

AP group's radio view

定義済みユーザーロール

network-admin

パラメータ

channelutilization: チャネル使用率に基づくアドミッションポリシーを指定します。

channelutilization-value: 最大チャネル使用率を 0～100%の範囲で指定します。デフォルトでは、最大チャネル使用率は 65%です。

client: クライアントベースのアドミッションポリシーを指定します。

client-number: 接続できるクライアントの最大数を 0～124 の範囲で指定します。

説明

cac policy コマンドは Connect Admission Control（CAC）ポリシーを設定します。

undo cac policy コマンドはデフォルトに戻します。

radio view の設定は、AP group’s radio view の設定よりも優先されます。

CAC ポリシーは、AC-VO キューおよび AC-VI キューでのみ有効です。

例

CAC のチャネル使用率に基づくアドミッションポリシーを設定し、最大チャネル使用率を 70%に設定します。

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] cac policy channelutilization 70

CAC のチャネル使用に基づくアドミッションポリシーを設定し、AP group apgroup1 の最大チャネル使用率を 70%に設定します。

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1110

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1]

cacpolicy channelutilization 70

3.1.4 client-rate-limit (radio view/AP group's radio view)

Syntax

client-rate-limit { **inbound** | **outbound** } **mode** {**dynamic cir** *cir* [**min** *min-cir*] [**max** *max-cir*]|**static cir** *cir* }

undo client-rate-limit { **inbound** | **outbound** }

View

Radio view

AP group’s radio view

定義済みユーザーロール

network-admin

パラメータ

inbound:受信トラフィックレートをリミットします。

outbound: 送信トラフィックレートをリミットします。

dynamic: ダイナミックレートリミットモードを指定します。このモードでは、各クライアントの最大レートは、合計最大レートをクライアント数で割った値になります。

static: スタティックレートリミットモードを指定します。各クライアントの最大レートは固定です。

cir *cir*:クライアントレートリミットを設定します。スタティックモードでは、すべてのクライアントに同じレートリミットが設定されます。ダイナミックモードでは、設定されているすべてのクライアントレートリミットの合計を示します。cir の範囲は 16～1700000 であり、単位は Kbps です。

min *min-cir*:すべてのクライアントの最小 CIR を設定します。min-cir の値の範囲は 16~1700000 で、単位は Kbps です。

max *max-cir*:すべてのクライアントの最大 CIR を設定します。max-cir は Kbps で 16~1700000 の値をとり、max-cir は min-cir より大きく設定する必要があります。

説明

client-rate-limit コマンドは無線ベースのクライアントレートリミットを設定します。

undo client-rate-limit コマンドはデフォルトに戻します。

このコマンドを有効にするには、無線ベースのクライアントレートリミットが有効になっていることを確認します。

このコマンドを複数回繰り返すことで、着信と発信トラフィックの両方のレートをリミットできます。

ダイナミックレートリミットに最小 CIR と最大 CIR の両方を指定すると、機能は次のように動作します。

- 指定した CIR をクライアントの総数で割った値が最小 CIR より小さい場合、最小 CIR はクライアントごとに有効になります。
- 指定した CIR をクライアントの総数で割った値が最大 CIR より大きい場合、最大 CIR はクライアントごとに有効になります。
- 指定した CIR をクライアントの総数で割った値が最小 CIR と最大 CIR の間にある場合、指定した CIR をクライアントの総数で割った値がクライアントごとに有効になります。

radio view の設定は、AP グループの radio view では設定よりも優先されます。

例

#単一のクライアントが送信するデータの最大レートが 567 Kbps で、すべてのクライアントが受信するデータの合計レートが 89 Kbps になるように、クライアントレートリミット機能を設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-1] client-rate-limit enable

[Sysname-wlan-ap-ap1-1] client-rate-limit inbound mode static cir 567

[Sysname-wlan-ap-ap1-1] client-rate-limit outbound mode dynamic cir 89

#単一のクライアントが送信するデータの最大レートが 567 Kbps で、すべてのクライアントが受信するデータの合計レートが 89 Kbps になるように、クライアントレートリミット機能を設定します。(AP group Radi view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1110

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1]client-rate-limit enable

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1]client-rate-limit inbound mode static cir 567

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1]client-rate-limit outbound mode dynamic cir 89

関連コマンド

- **client-rate-limit {disable | enable}**

3.1.5 client-rate-limit (service template view)

Syntax

client-rate-limit { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*

undo client-rate-limit { **inbound** | **outbound** }

デフォルト

設定なし

View

Service template view

定義済みユーザーロール

network-admin

パラメータ

inbound:受信トラフィックのレートを制限します。

outbound: 送信トラフィックのレートを制限します。

dynamic: ダイナミックレートリミットモードを指定します。このモードでは、各クライアントの最大レートは、合計最大レートをクライアント数で割った値になります。

cir *cir*:クライアントのレートリミットを設定します。スタティックモードでは、すべてのクライアントに同じレートリミットが設定されます。ダイナミックモードでは、設定されているすべてのクライアントのレートリミットの合計を示します。cir の範囲は 16～1700000 であり、単位は Kbps です。

min *min-cir*:すべてのクライアントの最小レートリミットを設定します。min-cir の値の範囲は 16~1700000 で、単位は Kbps です。

max *max-cir*:すべてのクライアントのレートリミットの最大値を設定します。max-cir は 16~1700000Kbps の値をとり、max-cir は min-cir より大きく設定する必要があります。

static: スタティックレートリミットモードを指定します。各クライアントの最大レートは固定です。

cbs *cbs* : 各クライアントのバーストサイズを 1～268435bytes の範囲で設定します。このパラメータが指定されていない場合、cbs の値は cir の値に従って自ダイナミックに計算されます。

説明

client-rate-limit コマンドを使用して、ワイヤレスサービステンプレートに基づいてクライアントレートリミットを設定します。

undo client-rate-limit コマンドはデフォルトに戻します。

このコマンドを複数回繰り返すことで、着信と発信トラフィックの両方のレートを制限できます。

ダイナミックレートリミットに最小 CIR、最大 CIR、またはその両方を指定した場合、この機能は次のように動作します。

- 指定した CIR をクライアントの総数で割った値が最小 CIR より小さい場合、最小 CIR はクライアントごとに有効になります。
- 指定した CIR をクライアントの総数で割った値が最大 CIR より大きい場合、最大 CIR はクライアントごとに有効になります。
- 指定した CIR をクライアントの総数で割った値が最小 CIR と最大 CIR の間にある場合、計算値はクライアントごとに有効になります。

例

すべてのクライアントが送信する合計データレートが 567Kbps、1 つのクライアントの最大送信レートが 500Kbps、最小送信レートが 123Kbps、すべてのクライアントが受信するデータの合計レートが 789Kbps になるように、クライアントレートリミット機能を設定します。単一クライアントの最大送信レート受信レートは 600Kbps、最小受信レートは 234Kbps です。

<Sysname> system-view

[Sysname] wlan service-template 1

[Sysname-wlan-st-1] client-rate-limit inbound mode dynamic cir 567 max 500 min 123

[Sysname-wlan-st-1] client-rate-limit outbound mode dynamic cir 789 max 600 min 234

3.1.6 client-rate-limit { disable | enable }

Syntax

client-rate-limit {**disable** |**enable** }

undo client-rate-limit

デフォルト

radio view は、AP group view の設定を使用します。

AP group's radio view は、無線ベースのクライアントレートリミットが無効になっています。

View

Radio view

AP group's radio view

定義済みユーザーロール

network-admin

説明

lient-rate-limit enable コマンドは無線ベースのクライアントレートリミットを有効にします。

client-rate-limit disable コマンドは無線ベースのクライアントレートリミットを無効にします。

undo client-rate-limit コマンドはデフォルトに戻します。

このコマンドは、無線に関連付けられた WLAN クライアントのトラフィックレートを制限します。レートリミット方向とレートリミットを設定するには、**client-rate-limit{inbound|outbound}**コマンドを使用します。

クライアントのレート制限にはさまざまなレートリミット方式とレートリミットモードを設定でき、すべての設定が有効になります。これらの設定の最小値は、各クライアントに適用されます。

radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#無線周波数ベースのクライアントレートリミットを有効にします。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] client-rate-limit enable

#無線周波数ベースのクライアントレートリミットを有効にします。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1110

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1]client-rate-limit enable

関連コマンド

- **client-rate-limit** (radio view/AP group's radio view)

3.1.7 display wlan wmm

Syntax

display wlan wmm {**client** [**ap** *ap-name* |**mac-address** *mac-address*]|**radio** [**ap** *ap-name*]}

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

client : WMM クライアントの統計を表示します。ap および mac-address パラメータが指定されていない場合、すべての WMM クライアントの統計が表示されます。

radio : WMM 無線の統計を表示します。ap パラメータが指定されていない場合、すべての WMM 無線の統計が表示されます。

ap *ap-name*: 指定された AP の WMM クライアントまたは WMM 無線統計を表示します。ap-name は AP の名前で、1 ～ 64 文字の文字列で、文字、数字、アンダースコア、「.」、「[」、「]」、「/」、および「-」を使用でき、大文字と小文字を区別します。

mac-address *mac-address*：指定された MAC アドレスの WMM クライアント統計を表示します。mac-address の形式は H-H-H です.

説明

display wlan wmm コマンドを使用して、WMM の統計情報を表示します。

例

#すべての AP の WMM 統計情報を表示します。

<Sysname> display wlan wmm radio

```
AP ID :4AP name :ap 1

Radio :1
Client EDCA updates :0
QoS mode  :WMM
WMM status    :Enabled
Radio max AIFSN:15Radio max ECWmin :10
Radio max TXOPLimit :32767Radio max ECWmax :10
CAC information
Clients accepted:0
Voice:0
Video:0
Total request medium time (μs):0
Voice (μs):0
Video (μs):0
Calls rejected due to insufficient resources:0
Calls rejected due to invalid parameters:0
Calls rejected due to invalid medium time:0
Calls rejected due to invalid delay bound:0

Radio :2
Client EDCA updates :0
QoS mode  :WMM
```

```
WMM status    :Disabled
Radio max AIFSN:15Radio max ECWmin :10
Radio max TXOPLimit :32767Radio max ECWmax :10
CAC information
Client accepted:0
Voice:0
Video:0
Total request medium time (μs):0
Voice (μs):0
Video (μs):0
Calls rejected due to insufficient resources:0
Calls rejected due to invalid parameters:0
Calls rejected due to invalid medium time:0
Calls rejected due to invalid delay bound:0
```

表 3-1 コマンド出力

フィールド	説明
Client EDCA updates	クライアントEDCAパラメータの更新回数
QoS mode	QoSモード: ● WMM:QoSモードはWMMです。 ● N/A:QoSモードは使用できません
WMM status	WMM機能のオン状態は、次の値を取ります。 ● Enabled:WMM機能がオンになっています ● Disabled:WMM機能がオフになっています
Radio max AIFSN	無線がサポートするAIFSN値の最大値です。
Radio max ECWmin	無線がサポートするECWmin値の最大値です。
Radio max TXOPLimit	無線がサポートするTXOPLimit値の最大値です。
Radio max ECWmax	無線がサポートするECWmax値の最大値です。
Total request medium time	AC-VOおよびAC-VIキューの合計要求中間時間(マイクロ秒)です。

#すべてのクライアントの WMM 統計情報を表示します。

<Sysname> display wlan wmm client

```
MAC address :000 f-e23c-0001SSID :service
QoS mode :WMM
APSD information :
Max SP length :7
L:LegacyT:TriggerD:Delivery
ACAC-BKAC-BEAC-VIAC-VO
Assoc StateT|DLT|DT|D
```

```
Statistics information :
Uplink packets:0Downlink packets:0
Uplink bytes:0Downlink bytes:0
Downgrade packets:0Discarded packets:0
Downgrade bytes:0Discarded bytes:0
TS information :
AC:AC-VOUser priority:7
TID:1Direction:Bidirectional
PSB:0Surplus bandwidth allowance :1.0000
Medium time (μs):39MSDU size (bytes):1500
Mean data rate (Kbps):10.000Minimum PHY rate (Mbps):11.000
TS creation time:0 h:0 m:5 s
TS updating time:0 h:0 m:5 s
Uplink TS packets:0Downlink TS packets:0
Uplink TS bytes:0Downlink TS bytes:0
```

表 3-2 コマンド出力

フィールド	説明
QoS mode	QoSモード: ● WMM ● N/A
Max SP length	最大サービス期間(Service period)の長さです。
AC	アクセスクラス: ● AC-VO ● AC-VI ● AC-BE ● AC-BK:
Assoc state	ACキューのAPSD属性 ● **T**－ACキューがtrigger-enabledです。 ● **D**－ACキューがdelivery-enabledです。 ● **T**	**D**－ACキューは、trigger-enabledとdelivery-enabledの両方です。 ● **L**－ACはレガシー属性のものです。
User priority	ユーザー優先順位(有線ネットワークからのパケット)
TID	0~15の範囲のトラフィックID
Direction	フロー方向には、次の値があります。 ● Uplink:上りです。 ● Downlink:下りです。 ● Bidirectional:双方向です。

フィールド	説明
PSB	省電力モードID (power save behavior): • 1はU-APSD省電力モードです。 • 0は従来の省電力モードです。
Surplus bandwidth allowance	使用可能な帯域幅(パーセント)です。
Medium time	許容される中間時間 (マイクロ秒) 。
MSDU size	平均パッケットサイズ(バイト)です。
Mean data rate	平均データ転送レート(Kbps)です。
Minimum PHY rate	最小物理転送レート (Mbps)です。

関連コマンド

- reset wlan wmm

3.1.8 edca client (ac-be and ac-bk)

Syntax

edca client { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax ecwmax-value** | **txoplimit** txoplimit-value }*

undo edca client { **ac-be** | **ac-bk** }

デフォルト

radio view は、AP group view で設定を使用します。

AP group's radio view で使用される、クライアントの AC-BE キューと AC-BK キューのデフォルトの EDCA パラメータ値をデフォルトの EDCA パラメータ値デフォルトの EDCA パラメータ値に示します。

表 3-3 デフォルトの EDCA パラメータ値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	10	0

View

Radio view

AP group view

定義済みユーザーロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を指数形式で 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）を指数形式で 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

txoplimit *txoplimit-value*: TXOP Limit（transmission opportunity limit）値を 0～65535（32 マイクロ秒単位）の範囲で指定します。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つの MPDU しか送信できません。

説明

edca client コマンドはクライアントの AC-BE キューまたは AC-BK キューの EDCA パラメータを設定します。

undo edca client コマンドはデフォルトに戻します。

radio view の設定は、AP group's radio view の設定よりも優先されます。

すべてのクライアントが 802.11b クライアントである場合、AC-BE キューと AC-BK キューのそれぞれに対して TXOP Limit 値を 0 に設定することを推奨します。

802.11b と 802.11g の両方のクライアントが WLAN に存在する場合、AC-BK と AC-BE のそれぞれのキューにデフォルトの TXOPLimit 値を使用することを推奨します。

例

AC-BE キューの AIFSN を 5 に設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] radio 1

AP group apgroup1 の AC-BE キューに対して AIFSN を 5 に設定します。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1110

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1] edca client ac-be aifsn 5

3.1.9 edca client (ac-vi and ac-vo)

Syntax

edca client { **ac-vi** | **ac-vo** } { **aifsn** *aifsn-value* | **cac** { **disable** | **enable** } | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo edca client { **ac-vi** | **ac-vo** }

デフォルト

radio view は、AP group view で設定を使用します。

AP group's radio view で使用される、クライアントの AC-VI キューと AC-VO キューのデフォルトの EDCA パラメータ値をデフォルトの EDCA パラメータ値に示します。

表 3-4 デフォルトの EDCA パラメータ値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-VI	2	3	4	94
AC-VO	2	2	3	47

View

Radio view

AP group's radio view

定義済みユーザーロール

network-admin

パラメータ

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

cac: CAC を指定します。AC-VO および AC-VI キューは CAC をサポートします。CAC はデフォルトで無効になっています。

disable: CAC を無効にします。

enable: CAC を有効にします。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を指数形式で 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）を指数形式で 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

txoplimit txoplimit-value: TXOP Limit（transmission opportunity limit）値を 0～65535（32 マイクロ秒単位）の範囲で指定します。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つの MPDU しか送信できません。

説明

edca client コマンドはクライアントの AC-VI または AC-VO キューの EDCA パラメータを設定します。

undo edca client コマンドはデフォルトに戻します。

radio view の設定は、AP group's radio view の設定よりも優先されます。

すべてのクライアントが 802.11b クライアントである場合、AC-VI および AC-VO キューの TXOPLimit 値をそれぞれ 188 と 102 に設定することを推奨します。

802.11b と 802.11g のそれぞれのクライアントが WLAN に存在する場合、AC-VI と AC-VO のそれぞれのキューにデフォルトの TXOPLimit 値を使用することを推奨します。

例

AC-VO キューの AIFSN を 3 に設定します。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] edca client ac-vo aifsn 3# AP group apgroup1 の AC-VO キューの AIFSN を 3 に設定します。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1110

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1] edca client ac-vo aifsn 3

3.1.10 edca radio

Syntax

edca radio { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** } { **ack-policy** { **noack** | **normalack** } | aifsn *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **noack** | **txoplimit** *txoplimit-value* } *

undo edca radio { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** }

デフォルト

radio view は、AP group view の設定を使用します。

AP group's radio view は、デフォルトの EDCA パラメータ値をデフォルトの EDCA パラメータ値に示します。

表 3-5 デフォルトの EDCA パラメータ値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	6	0
AC-VI	1	3	4	94
AC-VO	1	2	3	47

View

Radio vew

AP group's radio view

定義済みユーザーロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

ack-policy: AC キューの ACK ポリシーを指定します。

noack: No ACK ポリシー（デフォルト）を指定します。

normalack: Normal ACK ポリシーを指定します。

aifsn *aifsn-value*: AIFSN（Arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）の指数形式を指定します。*ecwmin-value* 引数の値の範囲は 0～10 です。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）の指数形式を指定します。*ecwmax-value* 引数の値の範囲は 0～10 です。ECWmax の値は ECWmin の値より小さくすることはできません。

txopimit *txoplimit-value*: TXOP Limit（Transmission opportunity limit）の値を 32 マイクロ秒単位で指定します。txoplimit-value 引数の値の範囲は 0～32767 です。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つの MPDU のみを送信できます。

説明

edca radio コマンドは EDCA パラメータを設定します。

undo edca radio コマンドはデフォルトに戻します。

radio view の設定は、AP group's radio view の設定よりも優先されます。

例

無線 2 の radio view で、AC-VO キューの AIFSN を 2 に設定します。

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] edca radio ac-vo aifsn 2

#AP group apgroup1 の無線 2 の radio view で、AC-VO キューの AIFSN を 2 に設定します。

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1110

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1] edca radio ac-vo aifsn 2

3.1.11 qos priority

Syntax

qos priotity *priority-value*

undo qos priotity

デフォルト

0

View

WLAN service template view

定義済みユーザーロール

network-admin

パラメータ

priority-value: ポートプライオリティを 0～7 の範囲で指定します。値が大きいほど優先度が高くなります。

説明

qos priority コマンドはポートプライオリティを設定します。

undo qos priority コマンドはデフォルトに戻します。

デバイスはポートプライオリティに基づいて適切なプライオリティを割り当てます。

パケットトラステッドモードが有効な場合このコマンドは有効になりません。

例

#ワイヤレスサービステンプレート 1 のポートプライオリティを 2 に設定します。

<Sysname> system

[Sysname] wlan service-template 1

[Sysname-wlan-st-1] qos priority 2

関連コマンド

- qos trust

3.1.12 qos trust

Syntax

qos trust [**dot11e** | **dscp**]

undo qos trust

デフォルト

ポートプライオリティを使用する。

View

WLAN service template view

定義済みユーザーロール

network-admin

パラメータ

dot11e: 優先度マッピングのためにパケット内で運ばれる 802.11e 優先度を使用します。
dscp: 優先度マッピングのためにパケット内で運ばれる DSCP 優先度を使用します。

説明

qos trust コマンドはパケットトラステッドモードを有効にします。

undo qos trust コマンドはデフォルトに戻します。

この機能は、アップリンクパケットでのみ有効です。

WLAN service template で優先度が設定してある場合はその優先度に従って優先度マッピングを行います。設定されていない場合はポートプライオリティに基づいて優先度マッピングを行います。

例

#プライオリティマッピングのために 802.11 パケットで伝送される 8002.11e プライオリティを使用するように WLAN service template1 を設定します。

<Sysname> system

[Sysname] wlan service-template 1

[Sysname-wlan-st-1] qos trust dot11e

関連コマンド

- qos priority

3.1.13 reset wlan wmm

Syntax

reset wlan wmm {**client** [**ap** *ap-name* |**mac-address** *mac-address*] | **radio** [*ap ap-name*] }

View

User view

定義済みユーザーロール

network-admin

パラメータ

client: クライアントの WMM 統計情報を削除します。

radio: 無線の WMM 統計情報を削除します。

ap ap-name: 指定した AP の WMM クライアントまたは WMM RF 統計情報を削除します。AP を名前で指定します。大文字と小文字を区別しない 1～64 文字です。文字列には、文字、数字、アンダースコア（_）、ドット（.）、左カッコ（[）、右カッコ（]）、スラッシュ（/）、ハイフン（-）を使用できます。

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H 形式で指定します。

説明

reset wlan wmm コマンドは WMM 統計情報を削除します。

例

#すべての無線の WMM 統計情報を削除します。

<Sysname> reset wlan wmm radio

関連コマンド

- display wlan wmm

3.1.14 svp map-ac

Syntax

svp map-ac { **ac-vi** | **ac-vo** }

svp map-ac disable

undo svp map-ac

デフォルト

radio view は、AP group view の設定を使用します。

AP group's radio view は、SVP マッピングが無効になっています。

View

Radio view

AP group's radio view

定義済みユーザーロール

network admin

パラメータ

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

説明

svp map-ac コマンドは指定された AC キューへの SVP マッピングを有効にします。

svp map-ac disable コマンドは SVP マッピングを無効にします。

undo svp map-ac コマンドはデフォルトに戻します。

SVP マッピングは、WMM 以外のクライアントでのみ有効です。

radio view の設定は、AP group's radio view の設定よりも優先されます。

例

#AC-VO キューの SVP マッピングを有効にして、SVP メッセージを AC-VO キューに入れます。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] svp map-ac ac-vo

#AC-VO キューの SVP マッピングを有効にして、SVP メッセージを AC-VO キューに入れます。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1110

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1] svp map-ac ac-vo

3.1.15 u-apsd enable

Syntax

u-apsd enable

undo u-apsd enable

デフォルト

有効

View

Service template view

定義済みユーザーロール

network admin

説明

U-APSD を有効にするには、**u-apsd enable** を使用します。

U-APSD を無効にするには、**undo u-apsd enable** を使用します。

スケジュールされていない自動省電力配信 (U-APSD) は、クライアントの省電力機能をさらに強化するために WMM によって定義された新しい省電力メカニズムです。

クライアントが U-APSD をサポートしている場合は、この機能を有効にしてクライアントの省電力機能を向上させることをお勧めします。

このコマンドは、サービステンプレートが無効になっている場合に設定できます。

例

U-APSD を有効に設定します。

<Sysname> system-view

[Sysname] wlan service-template service1

[Sysname-wlan-st-service1] u-apsd enable

3.1.16 wlan client-rate-limit

Syntax

wlan client-rate-limit { **dot11a** | **dot11ac** | **dot11an** | **dot11b** |**dot11g** | **dot11gac** |**dot11gn** | **dot11ax** | **dot11gax** } {**wlan client-rate-limit** |**dot11a** } **dot11ac** [**dot11an**]

undo wlan client-rate-limit [{ **dot11a** | **dot11ac** | **dot11an** | **dot11b** | **dot11g** | **dot11gac** | **dot11gn** | **dot11ax** | **dot11gax** } [**undo wlan client-rate-limit** | **dot11a**]]

デフォルト

設定なし

View

System view

定義済みユーザーロール

network-admin

パラメータ

dot11a:802.11 a クライアントを指定します。

dot11ac:802.11 ac クライアントを指定します。

dot11an:802.11 an クライアントを指定します。

dot11b:802.11 b クライアントを指定します。

dot11g:802.11 g クライアントを指定します。

dot11gac:802.11 gac クライアントを指定します。

dot11gn:802.11 gn クライアントを指定します。

dot11ax:802.11 ax クライアントを指定します。

dot11gax:802.11 gax クライアントを指定します。

inbound:受信トラフィックのレートをリミットします。

outbound: 送信トラフィックのレートをリミットします。

cir *cir*: 各クライアントの CIR を Kbps 単位で指定します。cir 引き数の値は 1～2097152 の範囲です。

cbs *cbs*: 各クライアントの CBS をバイト単位で指定します。cbs 引数の値は 1～268435456 の範囲です。このオプションを指定しない場合、CBS の値は CIR の値から自ダイナミックに計算されます。

説明

wlan client-rate-limit コマンドはユーザカテゴリに基づいてレートリミットを設定します。

undo wlan client-rate-limit コマンドはレートリミットを解除します。

クライアントレートリミットのために、異なるレートリミット方式とレートリミットモードを設定することができ、すべての設定が有効になります。これらの設定間のうちレートリミットの最小値が各クライアントに適用されます。

例

802.11an クライアントの受信トラフィックのレートリミットを 20480 Kbps に設定します。

<AC> system-view

[AC] wlan client-rate-limit dot11an inbound cir 20480

3.1.17 wlan max-bandwidth

Syntax

wlan max-bandwidth { dot11a | dot11ac | dot11an | dot11b | dot11g | dot11gac | dot11gn | dot11ax | dot11gax } *bandwidth*

undo wlan max-bandwidth [dot11a | dot11ac | dot11an | dot11b | dot11g | dot11gac | dot11gn | dot11ax | dot11gax]

デフォルト

- dot11a and dot11g：30000 Kbps
- dot11an, dot11gn, dot11gac, and dot11gax：250000 Kbps
- dot11ac ：500000 Kbps
- dot11ax ：700000 Kbps
- dot11b ：7000 Kbps

View

System view

定義済みユーザーロール

network admin

パラメータ

dot11a:802.11a 無線モードを指定します。

dot11ac:802.11ac 無線モードを指定します。

dot11an:802.11n (5 GHz) 無線モードを指定します。

dot11b:802.11b 無線モードを指定します。

dot11g:802.11g 無線モードを指定します。

dot11gac:802.11gac 無線モードを指定します。

dot11gn:802.11n (2.4 GHz) 無線モードを指定します。

dot11ax:802.11ax 無線モードを指定します。

dot11gax:802.11gax 無線モードを指定します。

bandwidth:最大帯域幅を Kbps 単位で指定します。値の範囲は、無線モードによって次のように異なります。

- dot11a および dot11g の場合は 16 から 30000。
- dot11an、dot11gn、dot11gac、および dot11gax の場合は 16 から 250000。
- dot11ac の場合は 16 から 500000。
- dot11ax の場合は 16 から 700000。
- dot11b の場合は 16 から 7000。

説明

無線モードの最大帯域幅を設定するには、**wlan max-bandwidth** を使用します。

1 つの無線モードまたはすべての無線モードのデフォルト設定を復元するには、**undo wlan max-bandwidth** を使用します。

最大帯域幅は、保証帯域幅の計算に使用されます。

例

802.11ac の最大帯域幅を 2000 Kbps に設定します。

<Sysname> system-view

[Sysname] wlan max-bandwidth dot11ac 2000

3.1.18 wmm

Syntax

wmm { **disable** | **enable** }

undo wmm

デフォルト

radio view は、AP group view で設定を使用します。

AP group’s radio view は、WMM が有効になっています。

View

Radio view

AP group’s radio view

定義済みユーザーロール

network-admin

パラメータ

disable: WMM を無効にします。

enable: WMM を有効にします。

説明

wmm enable コマンドは WMM を有効にします。

wmm disable コマンドは WMM を無効します。

undo wmm コマンドはデフォルトに戻します。

radio view の設定は、AP group's radio view の設定よりも優先されます。

802.11 n、802.11 ac、または 802.11 ax クライアントは WLAN QoS をサポートする必要があるため、802.11 an、802.11 gn、802.11 ac、または 802.11 ax で Radio が動作している場合は、WMM 機能を有効にする必要があります。有効にしないと、関連付けられた 802.11 n、802.11 ac、または 802.11 ax のクライアントが通信できなくなる可能性があります。

例

#WMM 機能を無効にします。(Radio view)

<Sysname> system-view

[Sysname] wlan ap ap1 model QX-W1110

[Sysname-wlan-ap-ap1] radio 1

[Sysname-wlan-ap-ap1-radio-1] wmm disable

#WMM 機能を無効にします。(AP group's radio view)

<Sysname> system-view

[Sysname] wlan ap-group apgroup1

[Sysname-wlan-ap-group-apgroup1] ap-model QX-W1110

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110] radio 1

[Sysname-wlan-ap-group-apgroup1-ap-model-QX-W1110-radio-1] wmm disable

QX-W2300AC シリーズ アクセスコントローラ

コマンドマニュアル

17. ネットワーク管理と監視

本マニュアルは以下に示す章で構成されています。

01- システムの保守

02- システムのデバッグ

03-NQA

04-SNMP

05-RMON

06-NETCONF

07-プロセスモニタリングとメンテナンス

08-ポートミラーリング

09-パケットキャプチャ

10-NetMeister

目次

このセクションのページは **17-x-x** です。

1 章 システムの保守 1-1
1.1 システムの保守設定コマンド 1-1
1.1.1 ping 1-1
1.1.2 tracert 1-4

1章 システムの保守

1.1 システムの保守設定コマンド

1.1.1 ping

Syntax

ping [**ip**] [**-a** source-ip |**-c** count |**-f**|**-h** ttl |**-i** interface-type interface-number |**-m** interval |**-n**|**-p** pad |**-q**|**-r**|**-s** packet-size |**-t** timeout |**-tos** tos |**-v**]*host

View

すべての view

定義済みユーザロール

network-admin

パラメータ

ip:宛先ホスト名が i、ip、ipv、ipv 6、l、ls、または lsp の場合、宛先ホスト名と ping コマンドキーワードを区別します。たとえば、宛先ホスト名が ip の場合、ping ip ではなく ping ip ip ip の形式でコマンドを使用する必要があります。

-a *source-ip*:ICMP エコー要求の送信元 IP アドレスとしてデバイスの IP アドレスを指定します。このオプションを指定しない場合、ICMP エコー要求の送信元 IP アドレスは、発信インターフェースのプライマリ IP アドレスになります。

-c *count*:宛先に送信する ICMP エコー要求の数を指定します。値の範囲は 1~4294967295 で、デフォルトは 5 です。

-f:IP ヘッダーの 「Don't Fragment」 ビットを設定します。

-h ttl:ICMP エコー要求の TTL 値を指定します。値の範囲は 1 から 255 で、デフォルトは 255 です。

-i *interface-type interface-number*:ICMP エコー要求の送信元インターフェースを指定します。このオプションを指定しない場合、一致するルートの出力インターフェースのプライマリ IP アドレスが、ICMP エコー要求の送信元インターフェースとして使用されます。

-m *interval*:ICMP エコー要求を送信する間隔 (ミリ秒単位) を指定します。値の範囲は 1 から 65535 で、デフォルトは 200 です。

-n:ホスト引数のドメイン名解決を無効にします。host 引数が宛先のホスト名を表し、このキーワードが指定されていない場合、デバイスは host をアドレスに変換します。

-p *pad*:ICMP エコー要求の pad フィールドの値を 16 進数形式で 1~8 ビットで指定します。pad 引数の範囲は 0 から ffffffff です。指定した値が 8 ビット未満の場合は、値の前に 0 s を追加して 8 ビットに拡張します。たとえば、pad が 0 x 2 f として設定されている場

合、パケットの合計長がデバイスの要件を満たすように、パケットは 0 x 0000002 f でパディングされます。デフォルトでは、パディングされた値は 0 x 01 から 0 xff までで始まり、必要に応じて別のラウンドが再開されます (0 x 010203 ... feff 01 ....など) 。

-q:要約統計情報のみを表示します。このキーワードを指定しない場合、すべての ping 統計情報が表示されます。

-r:渡された ICMP エコー要求のホップ (最大 9) のアドレスを記録します。このキーワードを指定しない場合、ICMP エコー要求が渡したホップのアドレスは記録されません。

-s *packet-size*:ICMP エコー要求の長さ (バイト単位) を指定します (IP パケットヘッダと ICMP パケットヘッダを除く) 。値の範囲は 20 から 9600 で、デフォルトは 56 です。

-t *timeout*:ICMP エコー応答のタイムアウト時間 (ミリ秒単位) を指定します。値の範囲は 0 から 65535 で、デフォルトは 2000 です。送信元がタイムアウト内に ICMP エコー応答を受信しない場合、ICMP エコー応答はタイムアウトしたと見なされます。

-tos *tos*:ICMP エコー要求の ToS 値を指定します。値の範囲は 0 から 255 で、デフォルトは 0 です。

-v:非 ICMP エコー応答パケットを表示します。このキーワードを指定しない場合、非 ICMP エコー応答パケットは表示されません。

host:宛先の IP アドレスまたはホスト名を指定します。ホスト名は、大文字と小文字を区別しない 1 文字から 253 文字の文字列です。文字、数字、ハイフン (-) 、アンダースコア (_) 、ドット (.) などの特殊文字を含めることができます。) 。

説明

ping コマンドは IP ネットワーク内の宛先装置が到達可能かどうかを検証し、関連する統計情報を表示します。

ping コマンドで宛先ホストの名前を使用する場合、装置の DNS の設定を行う必要があります。そうでなければ ping コマンドは失敗します。

ホスト名で識別されるデバイスに ping を実行するには、最初にデバイスの DNS 設定を構成します。DNS 設定が設定されていない場合、ping 操作は失敗します。

ping コマンドを実行中、Ctrl+C を押下することで中止することができます。

例

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。

<AC> ping 1.1.2.2

```
Ping 1.1.2.2 (1.1.2.2):56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2:icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2:icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2:icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2:icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2:icmp_seq=4 ttl=254 time=1.991 ms

--- ping statistics for 1.1.2.2 ---
```

```
5 packet (s) transmitted, 5 packet (s) received, 0.0% packet loss
round-trip min/avg/max/std-dev =1.963/2.0 28/2.137/0.062 ms
```

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。統計情報のみを表示します。

<AC> ping -q 1.1.2.2

```
Ping 1.1.2.2 (1.1.2.2):56 data bytes, press CTRL_C to break

--- ping statistics for 1.1.2.2 ---
5 packet (s) transmitted, 5 packet (s) received, 0.0% packet loss
round-trip min/avg/max/std-dev =1.962/2.196/2.665/0.244 ms
```

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。パスの ICMP パケットが通過する Hop アドレスを表示します。

<AC> ping -r 1.1.2.2

```
Ping 1.1.2.2 (1.1.2.2):56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2:icmp_seq=0 ttl=254 time=4.685 ms
RR:1.1.2.1
1.1.2.2
1.1.1.2
1.1.1.1
56 bytes from 1.1.2.2:icmp_seq=1 ttl=254 time=4.834 ms(same route)
56 bytes from 1.1.2.2:icmp_seq=2 ttl=254 time=4.770 ms(same route)
56 bytes from 1.1.2.2:icmp_seq=3 ttl=254 time=4.812 ms(same route)
56 bytes from 1.1.2.2:icmp_seq=4 ttl=254 time=4.704 ms(same route)

--- ping statistics for 1.1.2.2 ---
5 packet (s) transmitted, 5 packet (s) received, 0.0% packet loss
round-trip min/avg/max/std-dev =4.68 5/4.76 1/4.834/0.058 ms
```

出力は以下のことを示します。

- 宛先装置へ到達可能です。
- ルートは 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2 です。

表 1-1 コマンド出力

フィールド	説明
Ping 1.1.2.2 (1.1.2.2):56 data bytes, press CTRL_C to break	IPアドレス1.1.2.2の装置に到達可能かどうかを検証します。各ICMPエコー要求のパケット長は56バイトです。pingを中止する場合、Ctrl+Cを押下します。

フィールド	説明
56 bytes from 1.1.2.2:icmp_seq=0 ttl=254 time=4.685 ms	IPアドレス1.1.2.2の装置からICMPエコー応答を受信しました。タイムアウト時間内にエコー応答がない場合、表示されません。 ● bytes—ICMPエコー応答のバイト数です。 ● icmp_seq—セグメントが紛失、順番が異常、繰り返しているかどうかを確認するために使用されるパケットシーケンスです。 ● ttl—ICMPエコー応答のTTLです。 ● time—応答時間です。
RR:	ICMPエコー要求を通過したルータです。遠いところから順番に表示されるため宛先にもっとも近いルータが最初に表示されます。
--- ping statistics for 1.1.2.2 ---	ping操作で送受信されたデータの統計情報です。
5 packet (s) transmitted	送信されたICMPエコー要求の数です。
5 packet (s) received	受信したICMP応答の数です。
0.0% packet loss	送信された要求メッセージの合計に対する未応答要求メッセージの割合です。
round-trip min/avg/max/std-dev =4.685/4.76 1/4.834/0.058 ms	最小、平均、最大、標準偏差の応答時間です。単位はミリ秒です。

1.1.2 tracert

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-t** *tos* | **-w** *timeout*] * *host*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

-a *source-ip*:プローブパケットの送信元 IP アドレスとしてデバイスの IP アドレスを指定します。このオプションを指定しない場合、プローブパケットの送信元 IP アドレスは発信インターフェースのプライマリ IP アドレスになります。

-f *first-ttl:*宛先に送信される最初のパケットの TTL を指定します。値の範囲は 1 から 255 で、デフォルトは 1 です。max-ttl 引数の値以下である必要があります。

-i *interface-type interface-number*:プローブパケットの送信元インターフェースを指定する。このオプションを指定しない場合、システムは一致するルートのルーティングテーブルまたは転送テーブルを検索し、そのルートの出力インターフェースをプローブパケットの送信元インターフェースとして使用します。

-m *max-ttl*:プローブパケットに許可される最大ホップ数を指定します。値の範囲は 1 から 255 で、デフォルトは 30 です。これは、最初の ttl 引数の値以上である必要があります。

-p *port*:宛先の無効な UDP ポートを指定します。値の範囲は 1 から 65535 で、デフォルトは 33434 です。

-q *packet-number*:ホップごとに送信するプローブパケットの数を指定します。値の範囲は 1 から 65535 で、デフォルトは 3 です。

-t *tos*:プローブパケットの ToS 値を指定します。値の範囲は 0 から 255 で、デフォルトは 0 です。

-w *timeout*:プローブパケットの応答パケットのタイムアウト時間をミリ秒単位で指定します。値の範囲は 1 から 65535 で、デフォルトは 5000 です。

*host:*宛先の IP アドレスまたはホスト名を指定します。ホスト名は、大文字と小文字を区別しない 1 文字から 253 文字の文字列です。文字、数字、ハイフン (-) 、アンダースコア (_) 、ドット (.) などの特殊文字を含めることができます。) 。

説明

tracert コマンドは IPv4 パケットが送信元から宛先に向かう間に通過するルートを追跡します。

ping コマンドでネットワークの故障を識別したのち、**tracert** コマンドで故障したノードの位置を見つけることができます。

tracert コマンドの出力情報には、パケットが送信元から宛先に向かう間に通過するすべてのルートの IP アドレスが含まれます。ICMP エラーメッセージで装置が応答しない場合、アスタリスク（*.*.*）が表示されます。（宛先が到達不能あるいは ICMP タイムアウト/宛先到達不能パケットの送信が無効であることを示します。）

Tracert 処理において、中間デバイスが ICMP 到達不能パケット処理機能を有効にしている場合 (ip unreachables enable コマンドを参照)、コマンドの実行結果に次の文字が表示された場合、宛先デバイスが到達不能であることを意味します。デバイスはパケットの送信を停止し、Tracert プロセスは停止します。

- !N:ネットワークに到達できないことを示します。
- !H:宛先ホストが到達不能であることを示す。
- !P:プロトコルが到達不能であることを示す(不明なプロトコル番号)。
- !F:フラグメンテーションが行われていないため、中間デバイスが到達不能であることを示します。
- !W:未知の宛先ホストが到達不能である、すなわち宛先ホストが存在しないことを示します。。

- !Q:宛先ネットワークに到達できない、つまり利用できないサービスタイプ(ネットワーク)であることを示します。
- !T:宛先ホストに到達できない、つまり利用不能なサービスタイプ(ホスト)であることを示します。
- !X:通信がフィルタリングポリシーにより禁止されていることを示す。
- !V:メッセージ優先度が src/dst/port 不許可の優先度である場合、メッセージの転送が許可されないことを示します。
- !C:メッセージの優先度は終了され、転送できないことを示します。

コマンドの実行中に<Ctrl+C>と入力すると、Tracert 操作が終了します。

例

パケットが送信元から宛先（IP アドレス 1.1.2.2）へ向かうルートを表示します。

<AC> tracert 1.1.2.2

```
traceroute to 1.1.2.2 (1.1.2.2)、 30 hops at most, 40 bytes each packet, press CTRL_C to break
11.1.1.2(1.1.1.2) 673 ms 425 ms 30 ms
21.1.2.2(1.1.2.2) [AS 100] 580 ms 470 ms 80 ms
```

表 1-2 コマンド出力

フィールド	説明
traceroute to 1.1.2.2 (1.1.2.2)	現在の装置からIPアドレスが1.1.2.2の装置へ向かうIPパケットのルートを表示します。
hops at most	プローブパケットの最大Hop数です。このフィールドを表示する場合、-mを指定する必要があります。
bytes each packet	プローブパケットのバイト数です。
press CTRL_C to break	tracertコマンドを実行中、中止する場合、Ctrl+Cを押下します。
21.1.2.2(1.1.2.2) [AS 100] 580 ms 470 ms 80 ms	TTLが2のプローブパケットの結果です。2番目のホップは以下の情報が含まれます。 ● 最初のHopのドメイン名です。ドメイン名が設定されていない場合、IPアドレスが表示されます。 ● ホップのIPアドレスです。IPアドレスは括弧で表示されます。 ● プローブパケットのラウンドトリップ時間です。 各プローブが送信したパケット数を表示する場合、-qを指定する必要があります。

目次

このセクションのページは **17-x-x** です。

2 章 システムのデバッグ 2-1
2.1 システムのデバッグ設定コマンド 2-1
2.1.1 debugging 2-1
2.1.2 display debugging 2-2

2章 システムのデバッグ

2.1 システムのデバッグ設定コマンド

2.1.1 debugging

Syntax

debugging *module-name* [*option*]

undo debugging { **all** | *module-name* [*option*] }

デフォルト

無効

View

User view

定義済みユーザロール

network-admin

パラメータ

module-name: arp、device のようなモジュール名を指定します。現在のモジュール名を表示する場合、**debugging** ?コマンドを使用します。

option: モジュールのデバッグオプションを指定します。オプションの番号と内容はモジュールによって異なります。サポートされるオプションを表示する場合、**debugging** *module-name* ?コマンドを使用します。

all: すべてのモジュールにデバッグを無効にします。

説明

debugging コマンドは指定したモジュールのデバッグを有効にします。

undo debugging コマンドは指定したモジュールあるいはすべてのモジュールのデバッグを無効にします。

注意

デバッグ情報の出力が多すぎると、システムの運用効率に影響を与えるため、ネットワーク障害を診断する際には、必要に応じて特定の機能モジュールのデバッグ スイッチをオンにすることをお勧めします (複数の機能モジュールのデバッグスイッチをオンにしないでください)。

このコマンドの実行後、デバイスは生成されたデバッグ情報をデバイスのインフォメーションセンター モジュールに送信します。インフォメーションセンターのパラメータを設定することにより、デバッグ情報の出力ルール (つまり、出力を許可するかどうかと出力方向)が最終的に決定されます。

例

デバイス管理モジュールのデバッグ スイッチをオンにします。

<Sysname> debugging dev

関連コマンド

- display debugging

2.1.2 display debugging

Syntax

display debugging [*module-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

module-name: モジュール名を指定します。現在のモジュール名を表示する場合、debugging ?コマンドを使用します。

説明

display debugging コマンドは有効になっているデバッグを表示します。

例

有効になっているすべてのデバッグを表示します。

<AC> display debugging

```
DEV debugging switch is on
```

関連コマンド

- debugging

目次

このセクションのページは **17-x-x** です。

3 章 NQA 3-1
3.1 NQA 設定コマンド 3-1
3.1.1 advantage-factor 3-1
3.1.2 codec-type 3-2
3.1.3 data-fill 3-2
3.1.4 data-size 3-4
3.1.5 description 3-5
3.1.6 destination ip 3-6
3.1.7 destination port 3-7
3.1.8 display nqa history 3-8
3.1.9 display nqa result 3-11
3.1.10 display nqa statistics 3-20
3.1.11 filename 3-30
3.1.12 frequency 3-31
3.1.13 history-record enable 3-32
3.1.14 history-record keep-time 3-33
3.1.15 history-record number 3-34
3.1.16 next-hop 3-35
3.1.17 nqa 3-36
3.1.18 nqa agent enable 3-37
3.1.19 nqa schedule 3-37
3.1.20 operation (FTP operation view) 3-39
3.1.21 operation (HTTP operation view/HTTPS template view) 3-40
3.1.22 password 3-41
3.1.23 probe count 3-43
3.1.24 probe packet-interval 3-44
3.1.25 probe packet-number 3-45
3.1.26 probe packet-timeout 3-46
3.1.27 probe timeout 3-47
3.1.28 reaction checked-element probe-fail (for trap) 3-48
3.1.29 reaction trap 3-49
3.1.30 resolve-target 3-51
3.1.31 route-option bypass-route 3-52
3.1.32 source interface (ICMP echo/UDP tracert operation view) 3-53
3.1.33 source ip 3-54
3.1.34 source port 3-55

3.1.35 statistics interval 3-56
3.1.36 statistics max-group 3-57
3.1.37 tos 3-58
3.1.38 ttl 3-59
3.1.39 type 3-60
3.1.40 url 3-61
3.1.41 username 3-63
3.1.42 Version (HTTP operation view, HTTP/HTTPS template view) 3-64
3.2 NQA サーバ設定コマンド 3-65
3.2.1 display nqa server 3-65
3.2.2 nqa server enable 3-66
3.2.3 nqa server tcp-connect 3-67
3.2.4 nqa server udp-echo 3-68

3章 NQA

3.1 NQA設定コマンド

3.1.1 advantage-factor

Syntax

advantage-factor *factor*

undo advantage-factor

デフォルト

0

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

factor: アドバンテージファクタを指定します。設定範囲は 0～20 です。

説明

advantage-factor コマンドは MOS（Mean Opinion Scores）値と ICPIF（Calculated Planning Impairment Factor）値をカウントするのに使用されるアドバンテージファクタを設定します。

undo advantage-factor コマンドはデフォルトに戻します。

音声品質の評価は、ユーザの音声品質の許容度に依存します。音声品質に高い許容度を持つユーザの場合、アドバンテージファクタの設定を行う **advantage-factor** コマンドを使用します。システムが ICPIF 値を計算する場合、音声品質の評価用に ICPIF と MOS の値を修正するため、アドバンテージファクタが取りはずされます。

例

音声テストのアドバンテージファクタを 10 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type voice

[Switch-nqa-admin-test-voice] advantage-factor 10

3.1.2 codec-type

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

デフォルト

G.711 A-law

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

g711a: G.711 A-law コーデックタイプを指定します。

g711u: G.711 μ-law コーデックタイプを指定します。

g729a: G.729 A-law コーデックタイプを指定します。

説明

codec-type コマンドは音声テストのコーデックタイプを設定します。

undo codec-type コマンドはデフォルトに戻します。

例

音声テストのコーデックタイプを **g729a** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type voice

[Switch-nqa-admin-test-voice] codec-type g729a

3.1.3 data-fill

Syntax

data-fill *string*

undo data-fill

デフォルト

00010203040506070809

View

ICMP/UDP echo operation view

Path jitter/UDP jitter/voice operation view

ICMP/TCP/UDP template view

定義済みユーザロール

network-admin

パラメータ

string: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

説明

data-fill コマンドは各プローブパケットのペイロードに埋め込まれる文字列を設定します。

undo data-fill コマンドはデフォルトに戻します。

ペイロード長が埋め込みデータより小さい場合、文字列の最初の部分を使用します。たとえば、埋め込みデータが **abcd** で、テストパケットのデータサイズが 3 バイトの場合、**abc** がパケットに埋め込まれます。

ペイロード長が埋め込みデータより大きい場合、一杯になるまで文字列を繰り返し埋め込みます。たとえば、埋め込みデータが **abcd** で、テストパケットのデータサイズが 6 バイトの場合、**abcdab** がパケットに埋め込まれます。

テストタイプに依存して文字列が埋め込まれます。

- ICMP エコーテストでは、設定された文字列は ICMP エコー要求の全ペイロードに埋め込まれます。
- UDP エコーテストでは、UDP パケットのペイロードの最初の 5 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- UDP ジッタテストでは、UDP パケットのペイロードの最初の 68 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- 音声テストでは、UDP パケットのペイロードの最初の 16 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- パスジッタテストでは、ICMP エコー要求のペイロードの最初の 4 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。

例

ICMP エコー要求のペイロードに埋め込まれる文字列 **abcd** を設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] data-fill abcd

TCP テンプレート view で、プローブパケットのペイロードに埋め込まれる文字列 **abcd** を指定します。

<Switch> system-view

[Switch] nqa template tcp tcptplt

[Switch-nqatplt-tcp-tcptplt] data-fill abcd

3.1.4 data-size

Syntax

data-size *size*

undo data-size

デフォルト

異なるテストのプローブパケットのデフォルトのペイロードサイズを表 3-1 に示します。

表 3-1 プローブパケットのデフォルトのペイロードサイズ

テストタイプ	コーデックタイプ	デフォルトサイズ（バイト）
ICMP echo	N/A	100
UDP echo	N/A	100
UDP jitter	N/A	100
UDP tracert	N/A	100
Path jitter	N/A	100
Voice	G.711 A-law	172
Voice	G.711 μ-law	172
Voice	G.729 A-law	32

View

ICMP/UDP echo operation view

UDP tracert operation view

Path jitter/UDP jitter/voice operation view

ICMP/UDP template view

定義済みユーザロール

network-admin

パラメータ

size: 各プローブパケットのペイロードサイズを指定します。以下に設定範囲を示します。

- ICMP エコーあるいは UDP エコーテストのプローブパケットの設定範囲は 20～65507 バイトです。
- UDP ジッタテストのプローブパケットの設定範囲は 68～65507 バイトです。
- 音声テストのプローブパケットの設定範囲は 16～65507 バイトです。

説明

data-size コマンドは各プローブパケットのペイロードサイズを設定します。

undo data-size コマンドはデフォルトに戻します。

例

各 ICMP エコー要求のペイロードサイズを 80 バイトに設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] data-size 80

ICMP テンプレート view で、各プローブパケットのペイロードサイズを 80 バイトに設定します。

<Switch> system-view

[Switch] nqa template icmp icmptplt

[Switch-nqatplt-icmp-icmptplt] data-size 80

3.1.5 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

すべての NQA operation view

すべての NQA template view

定義済みユーザロール

network-admin

パラメータ

text: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

説明

description コマンドはテストタイプや目的などの NQA テストの説明を設定します。

undo description コマンドは説明をデフォルトに戻します。

例

NQA テストの説明を **icmp-probe** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] description icmp-probe

ICMP テンプレート view で、NQA オペレーションの説明を **icmp-probe** に設定します。

<Switch> system-view

[Switch] nqa template icmp icmptplt

[Switch-nqatplt-icmp-icmptplt] description icmp-probe

3.1.6 destination ip

Syntax

destination ip *ip-address*

undo destination ip

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

DNS/ICMP/RADIUS/SSL/TCP/TCP half open/UDP template view

定義済みユーザロール

network-admin

パラメータ

ip-address: テストの宛先 IP アドレスを指定します。

説明

destination ip コマンドはテストの宛先 IP アドレスを設定します。

undo destination ip コマンドは宛先 IP アドレスをデフォルトに戻します。

例

ICMP エコーテストの宛先 IPv4 アドレスを 10.1.1.1 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] destination ip 10.1.1.1

ICMP テンプレート view で、ICMP エコーテストの宛先 IPv4 アドレスを 0.1.1.1 に指定します。

<Switch> system-view

[Switch] nqa template icmp icmptplt

[Switch-nqatplt-icmp-icmptplt] destination ip 10.1.1.1

3.1.7 destination port

Syntax

destination port *port-number*

undo destination port

デフォルト

宛先ポート番号は、UDP tracert テストの場合は 33434、SNMP テストの場合は 161 です。

次の NQA テンプレートを使用するテストの宛先ポート番号は、次のとおりです。

- DNS テンプレートの場合は 53 です。
- RADIUS テンプレートの場合は 1812 です。

他のタイプのテストでは、宛先ポート番号は設定されません。

View

TCP/UDP echo operation view

UDP tracert operation view

UDP jitter/voice operation view

DNS/RADIUS/SSL/TCP/UDP template view

定義済みユーザロール

network-admin

パラメータ

port-number: テストの宛先ポート番号を指定します。設定範囲は 1～65535 です。

説明

destination port コマンドはテストの宛先ポート番号を設定します。

undo destination port コマンドはデフォルトに戻します。

例

UDP エコーテストの宛先ポート番号を 9000 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type udp-echo

[Switch-nqa-admin-test-udp-echo] destination port 9000

TCP テンプレート view で、NQA オペレーションの宛先ポート番号を 9000 に設定します。

<Switch> system-view

[Switch] nqa template tcp tcptplt

[Switch-nqatplt-tcp-tcptplt] destination port 9000

3.1.8 display nqa history

Syntax

display nqa history [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの履歴記録を表示します。

説明

display nqa history コマンドは NQA テストの履歴記録を表示します。

display nqa history コマンドは次のテストの結果または統計情報は表示されません。

- フレームロス
- ICMP ジッタ
- 待ち時間
- パスジッタ
- スループット
- UDP ジッタ
- 音声

ICMP ジッタ、パスジッタ、UDP ジッタテストと音声テストを確認する場合、**display nqa result** コマンドあるいは **display nqa statistics** コマンドを使用します。

例

管理者名が **administrator**、オペレーティングタグが **tracert** の UDP tracert テストの履歴記録を表示します。

<Switch> display nqa history administrator tracert

```
NQA entry (admin administrator, tag tracert) history records:
Index     TTL  Response  Hop IP         Status         Time
1         2    328      4.1.1.1        Succeeded      2013-09-09 14:46:06.2
1         2    328      4.1.1.1        Succeeded      2013-09-09 14:46:05.2
1         2    328      4.1.1.1        Succeeded      2013-09-09 14:46:04.2
1         1    328      3.1.1.2        Succeeded      2013-09-09 14:46:03.2
1         1    328      3.1.1.1        Succeeded      2013-09-09 14:46:02.2
1         1    328      3.1.1.1        Succeeded      2013-09-09 14:46:01.2
```

管理者名が **administrator**、オペレーティングタグが **test** の NQA オペレーションの履歴記録を表示します。

<Switch> display nqa history administrator test

```
NQA entry (admin administrator, tag test) history records:
  Index      Response     Status          Time
  10         329          Succeeded       2011-04-29 20:54:26.5
  9          344          Succeeded       2011-04-29 20:54:26.2
  8          328          Succeeded       2011-04-29 20:54:25.8
  7          328          Succeeded       2011-04-29 20:54:25.5
  6          328          Succeeded       2011-04-29 20:54:25.1
  5          328          Succeeded       2011-04-29 20:54:24.8
  4          328          Succeeded       2011-04-29 20:54:24.5
  3          328          Succeeded       2011-04-29 20:54:24.1
  2          328          Succeeded       2011-04-29 20:54:23.8
  1          328          Succeeded       2011-04-29 20:54:23.4
```

表 3-2 コマンド出力

フィールド	説明
Index	履歴記録のIDです。 1つのUDP tracertテストの履歴記録に同じIDがあります。
TTL	テストでルーティングテーブルバイパス機能が有効になっていない場合、このフィールドにはプローブパケットのTTL値が表示されます。 ルーティングテーブルバイパス機能が有効な場合、このフィールドには**init-ttl**コマンドを使用して構成されたTTL値が表示されます。ただし、プローブパケット内の実際のTTL値は1に固定されています。
Response	テストが成功した場合、ラウンドトリップの時間を表示します。テストがタイムアウトしたとき、タイムアウト時間を表示します。テストが完了しない場合、0を表示します。単位はミリ秒です。
Hop IP	応答パケットを送信したノードのIPアドレスです。
Status	テスト結果の状態です。 ● **Succeeded**－成功しました。 ● **Unknown error**－未知のエラーです。 ● **Internal error**－内部エラーです。 ● **Timeout**－タイムアウトしました。
Time	テストが完了したときの時間です。

3.1.9 display nqa result

Syntax

display nqa result [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの最新の結果を表示します。

説明

display nqa result コマンドは NQA テストの最新の結果を表示します。

例

管理者名が **admin** で、テストタグが **test** である TCP テストの最新の結果を表示します。

<Switch> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
   Send operation times: 1            Receive response times: 1
   Min/Max/Average round trip time: 35/35/35
   Square-Sum of round trip time: 1225
   Last succeeded probe time: 2011-05-29 10:50:33.2
  Extended results:
   Packet loss ratio: 0%
   Failures due to timeout: 0
   Failures due to disconnect: 0
   Failures due to no connection: 0
   Failures due to internal error: 0
   Failures due to other errors: 0
```

管理者名が **admin** で、テストタグが **test** である ICMP ジッタテストの最新の結果を表示します。

<Switch> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
    Send operation times: 10          Receive response times: 10
    Min/Max/Average round trip time: 1/2/1
    Square-Sum of round trip time: 13
    Last packet received time: 2015-03-09 17:40:29.8
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  ICMP-jitter results:
   RTT number: 10
    Min positive SD: 0                Min positive DS: 0
    Max positive SD: 0                Max positive DS: 0
    Positive SD number: 0             Positive DS number: 0
    Positive SD sum: 0                Positive DS sum: 0
    Positive SD average: 0            Positive DS average: 0
    Positive SD square-sum: 0         Positive DS square-sum: 0
    Min negative SD: 1                Min negative DS: 2
    Max negative SD: 1                Max negative DS: 2
    Negative SD number: 1             Negative DS number: 1
    Negative SD sum: 1                Negative DS sum: 2
    Negative SD average: 1            Negative DS average: 2
    Negative SD square-sum: 1         Negative DS square-sum: 4
  One way results:
    Max SD delay: 1                   Max DS delay: 2
    Min SD delay: 1                   Min DS delay: 2
    Number of SD delay: 1             Number of DS delay: 1
    Sum of SD delay: 1                Sum of DS delay: 2
    Square-Sum of SD delay: 1         Square-Sum of DS delay: 4
    Lost packets for unknown reason: 0
```

管理者名が **admin** で、テストタグが **test** である UDP ジッタテストの最新の結果を表示します。

<Switch> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
    Send operation times: 10          Receive response times: 10
    Min/Max/Average round trip time: 15/46/26
    Square-Sum of round trip time: 8103
    Last packet received time: 2011-05-29 10:56:38.7
  Extended results:
```

```
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
 UDP-jitter results:
  RTT number: 10
  Min positive SD: 8                Min positive DS: 8
  Max positive SD: 18               Max positive DS: 8
  Positive SD number: 5             Positive DS number: 2
  Positive SD sum: 75               Positive DS sum: 32
  Positive SD average: 15           Positive DS average: 16
  Positive SD square-sum: 1189      Positive DS square-sum: 640
  Min negative SD: 8                Min negative DS: 1
  Max negative SD: 24               Max negative DS: 30
  Negative SD number: 4             Negative DS number: 7
  Negative SD sum: 56               Negative DS sum: 99
  Negative SD average: 14           Negative DS average: 14
  Negative SD square-sum: 946       Negative DS square-sum: 1495
 One way results:
  Max SD delay: 22                  Max DS delay: 23
  Min SD delay: 7                   Min DS delay: 7
  Number of SD delay: 10            Number of DS delay: 10
  Sum of SD delay: 125              Sum of DS delay: 132
  Square-Sum of SD delay: 1805      Square-Sum of DS delay: 1988
  SD lost packets: 0                DS lost packets: 0
  Lost packets for unknown reason: 0
```

 # 管理者名が admin で、テストタグが test である最新の音声テスト結果を表示します。

<Switch> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
  Send operation times: 1000        Receive response times: 0
  Min/Max/Average round trip time: 0/0/0
  Square-Sum of round trip time: 0
  Last packet received time: 0-00-00 00:00:00.0
 Extended results:
  Packet loss ratio: 100%
  Failures due to timeout: 1000
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
```

```
  Voice results:
   RTT number: 0
    Min positive SD: 0                  Min positive DS: 0
    Max positive SD: 0                  Max positive DS: 0
    Positive SD number: 0               Positive DS number: 0
    Positive SD sum: 0                  Positive DS sum: 0
    Positive SD average: 0              Positive DS average: 0
    Positive SD square-sum: 0           Positive DS square-sum: 0
    Min negative SD: 0                  Min negative DS: 0
    Max negative SD: 0                  Max negative DS: 0
    Negative SD number: 0               Negative DS number: 0
    Negative SD sum: 0                  Negative DS sum: 0
    Negative SD average: 0              Negative DS average: 0
    Negative SD square-sum: 0           Negative DS square-sum: 0
  One way results:
    Max SD delay: 0                    Max DS delay: 0
    Min SD delay: 0                    Min DS delay: 0
    Number of SD delay: 0               Number of DS delay: 0
    Sum of SD delay: 0                  Sum of DS delay: 0
    Square-Sum of SD delay: 0           Square-Sum of DS delay: 0
    SD lost packets: 0                  DS lost packets: 0
    Lost packets for unknown reason: 1000
  Voice scores:
    MOS value: 0.99                    ICPIF value: 87
```

 # 管理者名が admin で、テストタグが test であるパスジッタテストの最新の結果を表示します。

<Switch> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
  Hop IP 192.168.40.210
    Basic Results:
      Send operation times: 10
      Receive response times: 10
      Min/Max/Average round trip time: 1/1/1
      Square-Sum of round trip time: 10
    Extended Results:
      Packet loss ratio: 0%
      Failures due to timeout: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
      Packets out of sequence: 0
      Packets arrived late: 0
    Path-Jitter Results:
```

```
    Jitter number: 9
      Min/Max/Average jitter: 0/0/0
    Positive jitter number: 0
      Min/Max/Average positive jitter: 0/0/0
      Sum/Square-Sum positive jitter: 0/0
    Negative jitter number: 0
      Min/Max/Average negative jitter: 0/0/0
      Sum/Square-Sum negative jitter: 0/0
  Hop IP 192.168.50.209
    Basic Results:
    Send operation times: 10
    Receive response times: 10
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 10
    Extended Results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
    Path-Jitter Results:
    Jitter number: 9
      Min/Max/Average jitter: 0/0/0
    Positive jitter number: 0
      Min/Max/Average positive jitter: 0/0/0
      Sum/Square-Sum positive jitter: 0/0
    Negative jitter number: 0
      Min/Max/Average negative jitter: 0/0/0
      Sum/Square-Sum negative jitter: 0/0
```

管理者名が **admin** で、テストタグが **test** である UDP tracert テストの最新の結果を表示します。

<Switch> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
   Send operation times: 6            Receive response times: 6
   Min/Max/Average round trip time: 35/35/35
   Square-Sum of round trip time: 1225
   Last succeeded probe time: 2013-09-09 14:23:24.5
  Extended results:
   Packet loss ratio: 0%
   Failures due to timeout: 0
   Failures due to internal error: 0
```

```
  Failures due to other errors: 0
UDP-tracert results:
  TTL    Hop IP           Time
  1      3.1.1.1          2013-09-09 14:23:24.5
  2      4.1.1.1          2013-09-09 14:23:24.5
```

表 3-3 コマンド出力

フィールド	説明
Data collecting in progress	テストは進行中です。
Send operation times	テスト数です。
Receive response times	受信した応答パケットの数です。
Min/Max/Average round trip time	最小/最大/平均ラウンドトリップタイムです。単位はミリ秒です。
Square-Sum of round trip time	ラウンドトリップタイムの2乗和です。
Last succeeded probe time	連続した最後のプローブが完了した時間です。テストでプローブが連続していない場合、**0**と表示されます。 このフィールドはUDPジッタ、音声テストで無効です。
Last packet received time	連続した最後の応答パケットを受信した時間です。プローブで応答パケットを受信しない場合、**0**と表示されます。 このフィールドはUDPジッタ、音声テストで有効です。
Packet loss ratio	平均パケット損失レートです。
Failures due to timeout	テストでタイムアウトが発生した回数です。
Failures due to disconnect	ピアが切断した数です。
Failures due to no connection	ピアとの接続に失敗した数です。
Failures due to internal error	内部エラーによる故障の数です。
Failures due to other errors	他のエラーによる故障の数です。
Packets out of sequence	異なる順番のパケットによる故障の数です。
ICMP-jitter results	ICMPジッタテストの結果です。 このフィールドは、ICMPジッタテストのみ有効です。
Packets arrived late	プローブがタイムアウトしたのち応答パケットを受信した数です。
UDP-jitter results	UDPジッタテストの結果です。このフィールドはUDPジッタテストのみ有効です。

フィールド	説明
Voice results	音声テストの結果です。このフィールドは音声テストのみ有効です。
RTT number	応答パケットを受信した数です。
Min positive SD	送信元から宛先への最小ポジティブジッタです。
Min positive DS	宛先から送信元への最小ポジティブジッタです。
Max positive SD	送信元から宛先への最大ポジティブジッタです。
Max positive DS	宛先から送信元への最大ポジティブジッタです。
Positive SD number	送信元から宛先へのポジティブジッタの数です。
Positive DS number	宛先から送信元へのポジティブジッタの数です。
Positive SD sum	送信元から宛先へのポジティブジッタの合計数です。
Positive DS sum	宛先から送信元へのポジティブジッタの合計数です。
Positive SD average	送信元から宛先への平均ポジティブジッタです。
Positive DS average	宛先から送信元への平均ポジティブジッタです。
Positive SD square-sum	送信元から宛先へのポジティブジッタの2乗和です。
Positive DS square-sum	宛先から送信元へのポジティブジッタの2乗和です。
Min negative SD	送信元から宛先へのネガティブジッタの絶対値の最小値です。
Min negative DS	宛先から送信元へのネガティブジッタの絶対値の最小値です。
Max negative SD	送信元から宛先へのネガティブジッタの絶対値の最大値です。
Max negative DS	宛先から送信元へのネガティブジッタの絶対値の最大値です。
Negative SD number	送信元から宛先へのネガティブジッタの数です。
Negative DS number	宛先から送信元へのネガティブジッタの数です。
Negative SD sum	送信元から宛先へのネガティブジッタの絶対値の合計です。
Negative DS sum	宛先から送信元へのネガティブジッタの絶対値の合計です。

フィールド	説明
Negative SD average	送信元から宛先へのネガティブジッタの絶対値の平均です。
Negative DS average	宛先から送信元へのネガティブジッタの絶対値の平均です。
Negative SD square-sum	送信元から宛先へのネガティブジッタの2乗和です。
Negative DS square-sum	宛先から送信元へのネガティブジッタの2乗和です。
One way results	片方向遅延です。 このフィールドはUDPジッタテスト、音声テストで有効です。
Max SD delay	送信元から宛先への最大遅延です。
Max DS delay	宛先から送信元への最大遅延です。
Min SD delay	送信元から宛先への最小遅延です。
Min DS delay	宛先から送信元への最小遅延です。
Number of SD delay	送信元から宛先への遅延の数です。
Number of DS delay	宛先から送信元への遅延の数です。
Sum of SD delay	送信元から宛先への遅延の合計です。
Sum of DS delay	宛先から送信元への遅延の合計です。
Square-Sum of SD delay	送信元から宛先への遅延の2乗和です。
Square-Sum of DS delay	宛先から送信元への遅延の2乗和です。
SD lost packets	送信元から宛先への損失したパケット数です。
DS lost packets	宛先から送信元への損失したパケット数です。
Lost packets for unknown reason	不明な理由で損失したパケット数です。
Voice scores	音声パラメータです。 このフィールドは音声テストで有効です。
MOS value	音声テストの計算されたMOS値です。
ICPIF value	音声テストの計算されたICPIF値です。
Hop IP	ホップのIPアドレスです。 このフィールドは、パスジッタテストでのみ使用できます。

フィールド	説明
Path-jitter results	パスジッタのテスト結果です。 このフィールドは、パスジッタテストでのみ使用できます。
Jitter number	ジッタの数です。 このフィールドは、パスジッタテストでのみ使用できます。
Min/Max/Average jitter	最小/最大/平均ジッタです。単位はミリ秒です。 このフィールドは、パスジッタテストでのみ使用できます。
Positive jitter number	正のジッタの数です。 このフィールドは、パスジッタテストでのみ使用できます。
Min/Max/Average positive jitter	最小/最大/平均の正のジッタです。単位はミリ秒です。 このフィールドは、パスジッタテストでのみ使用できます。
Sum/Square-Sum positive jitter	正のジッタの和/2乗和です。 このフィールドは、パスジッタテストでのみ使用できます。
Negative jitter number	負のジッタの数です。 このフィールドは、パスジッタテストでのみ使用できます。
Min/Max/Average negative jitter	最小/最大/平均の負のジッタです。単位はミリ秒です。 このフィールドは、パスジッタテストでのみ使用できます。
Sum/Square-Sum negative jitter	負のジッタの和/2乗和です。 このフィールドは、パスジッタテストでのみ使用できます。
TTL	テストでルーティングテーブルバイパス機能が有効になっていない場合、このフィールドにはプローブパケットのTTL値が表示されます。 ルーティングテーブルバイパス機能が有効な場合、このフィールドには**init-ttl**コマンドを使用して構成されたTTL値が表示されます。ただし、プローブパケット内の実際のTTL値は1に固定されています。
Hop IP	応答パケットを送信したノードのIPアドレスです。
Time	NQAクライアントが応答パケットを受信した時刻です。

3.1.10 display nqa statistics

Syntax

display nqa statistics [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの統計情報を表示します。

説明

display nqa statistics コマンドは NQA テストの統計情報を表示します。

NQA テストが完了した後、統計情報が作成されます。テストが完了する前に **display nqa statistics** コマンドを実行した場合、統計情報はすべて 0 で表示されます。

リアクションエントリが設定されている場合、**statistics interval** コマンドで指定された期間、リアクションエントリをモニタリングした結果を表示します。しきい値タイプが平均値あるいは音声テストのモニタリングした性能の値が ICPIF あるいは MOS である場合、ハイフン（-）が結果として表示されます。

例

管理者名が **admin** で、operation タグが **test** である TCP テストの統計情報を表示します。

<Switch> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:30:20.0
    Life time: 2 seconds
    Send operation times: 1            Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
```

```
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
```

管理者名が admin で、operation tag test にある ICMP jitter operation の統計情報を表示します。

<Switch> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
 NO. : 1
  Start time: 2015-03-09 17:42:10.7
  Life time: 156 seconds
  Send operation times: 1560         Receive response times: 1560
  Min/Max/Average round trip time: 1/2/1
  Square-Sum of round trip time: 1563
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
 ICMP-jitter results:
  RTT number: 1560
  Min positive SD: 1                 Min positive DS: 1
  Max positive SD: 1                 Max positive DS: 2
  Positive SD number: 18              Positive DS number: 46
  Positive SD sum: 18                Positive DS sum: 49
  Positive SD average: 1              Positive DS average: 1
  Positive SD square-sum: 18          Positive DS square-sum: 55
  Min negative SD: 1                 Min negative DS: 1
  Max negative SD: 1                 Max negative DS: 2
  Negative SD number: 24              Negative DS number: 57
  Negative SD sum: 24                Negative DS sum: 58
  Negative SD average: 1              Negative DS average: 1
  Negative SD square-sum: 24          Negative DS square-sum: 60
 One way results:
  Max SD delay: 1                   Max DS delay: 2
  Min SD delay: 1                   Min DS delay: 1
  Number of SD delay: 4              Number of DS delay: 4
  Sum of SD delay: 4                 Sum of DS delay: 5
  Square-Sum of SD delay: 4           Square-Sum of DS delay: 7
  Lost packets for unknown reason: 0
```

```
  Reaction statistics:
    Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
    1      jitter-DS       accumulate      1500         10
    2      jitter-SD       average         -            -
    3      OWD-DS          -               1560         2
    4      OWD-SD          -               1560         0
    5      packet-loss      accumulate      0            0
    6      RTT             accumulate      1560         0
```

管理者名が **admin** で、operation タグが **test** である UDP ジッタテストの統計情報を表示します。

<Switch> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:33:22.3
    Life time: 23 seconds
    Send operation times: 100          Receive response times: 100
    Min/Max/Average round trip time: 1/11/5
    Square-Sum of round trip time: 24360
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 550
    Min positive SD: 1                 Min positive DS: 1
    Max positive SD: 7                 Max positive DS: 1
    Positive SD number: 220             Positive DS number: 97
    Positive SD sum: 283               Positive DS sum: 287
    Positive SD average: 1              Positive DS average: 2
    Positive SD square-sum: 709          Positive DS square-sum: 1937
    Min negative SD: 2                 Min negative DS: 1
    Max negative SD: 10                Max negative DS: 1
    Negative SD number: 81              Negative DS number: 94
    Negative SD sum: 556               Negative DS sum: 191
    Negative SD average: 6              Negative DS average: 2
    Negative SD square-sum: 4292         Negative DS square-sum: 967
  One way results:
    Max SD delay: 5                    Max DS delay: 5
    Min SD delay: 1                    Min DS delay: 1
```

```
  Number of SD delay: 550             Number of DS delay: 550
  Sum of SD delay: 1475               Sum of DS delay: 1201
  Square-Sum of SD delay: 5407         Square-Sum of DS delay: 3959
  SD lost packets: 0                 DS lost packets: 0
  Lost packets for unknown reason: 0
 Reaction statistics:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      jitter-DS       accumulate      90           25
  2      jitter-SD       average         -            -
  3      OWD-DS          -               100          24
  4      OWD-SD          -               100          13
  5      packet-loss      accumulate      0            0
  6      RTT             accumulate      100          52
```

管理者名が **admin** で、operation タグが **test** である音声テストの統計情報を表示します。

<Switch> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
 NO. : 1
  Start time: 2007-01-01 09:33:45.3
  Life time: 120 seconds
  Send operation times: 10           Receive response times: 10
  Min/Max/Average round trip time: 1/12/7
  Square-Sum of round trip time: 620
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
 Voice results:
  RTT number: 10
  Min positive SD: 3                 Min positive DS: 1
  Max positive SD: 10                Max positive DS: 1
  Positive SD number: 3              Positive DS number: 2
  Positive SD sum: 18                Positive DS sum: 2
  Positive SD average: 6             Positive DS average: 1
  Positive SD square-sum: 134          Positive DS square-sum: 2
  Min negative SD: 3                 Min negative DS: 1
  Max negative SD: 9                 Max negative DS: 1
  Negative SD number: 4              Negative DS number: 2
  Negative SD sum: 25                Negative DS sum: 2
```

```
  Negative SD average: 6              Negative DS average: 1
  Negative SD square-sum: 187         Negative DS square-sum: 2
 One way results:
  Max SD delay: 0                    Max DS delay: 0
  Min SD delay: 0                    Min DS delay: 0
  Number of SD delay: 0              Number of DS delay: 0
  Sum of SD delay: 0                 Sum of DS delay: 0
  Square-Sum of SD delay: 0          Square-Sum of DS delay: 0
  SD lost packets: 0                 DS lost packets: 0
  Lost packets for unknown reason: 0
 Voice scores:
  Max MOS value: 4.40                Min MOS value: 4.40
  Max ICPIF value: 0                 Min ICPIF value: 0
 Reaction statistics:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      ICPIF            -              -            -
  2      MOS              -              -            -
```

管理者名が **admin** で、operation タグが **test** であるパスジッタテストの統計情報を表示します。

<Switch> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
 NO. : 1
 Path 1:
 Hop IP 192.168.40.210
  Basic Results:
   Send operation times: 10
   Receive response times: 10
   Min/Max/Average round trip time: 1/1/1
   Square-Sum of round trip time: 10
  Extended Results:
   Packet loss ratio: 0%
   Failures due to timeout: 0
   Failures due to internal error: 0
   Failures due to other errors: 0
   Packets out of sequence: 0
   Packets arrived late: 0
  Path-Jitter Results:
   Jitter number: 9
    Min/Max/Average jitter: 0/0/0
   Positive jitter number: 0
    Min/Max/Average positive jitter: 0/0/0
    Sum/Square-Sum positive jitter: 0/0
```

```
    Negative jitter number: 0
      Min/Max/Average negative jitter: 0/0/0
      Sum/Square-Sum negative jitter: 0/0
Hop IP 192.168.50.209
  Basic Results:
    Send operation times: 10
    Receive response times: 10
    Min/Max/Average round trip time: 1/1/1
    Square-Sum of round trip time: 10
  Extended Results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  Path-Jitter Results:
    Jitter number: 9
      Min/Max/Average jitter: 0/0/0
    Positive jitter number: 0
      Min/Max/Average positive jitter: 0/0/0
      Sum/Square-Sum positive jitter: 0/0
    Negative jitter number: 0
      Min/Max/Average negative jitter: 0/0/0
      Sum/Square-Sum negative jitter: 0/0
```

表 3-4 コマンド出力

フィールド	説明
No.	統計情報のグループIDです。
Start time	テストが開始した時間です。
Life time	テストの所要時間です。
Send operation times	送信したプローブパケットの数です。
Receive response times	受信した応答パケットの数です。
Min/Max/Average round trip time	最小/最大/平均ラウンドトリップタイムです。単位はミリ秒です。
Square-Sum of round trip time	ラウンドトリップタイムの2乗和です。
Packet loss ratio	平均パケット損失レートです。

フィールド	説明
Failures due to timeout	テストでタイムアウトが発生した回数です。
Failures due to disconnect	ピアが切断した数です。
Failures due to no connection	ピアとの接続に失敗した数です。
Failures due to internal error	内部エラーによる故障の数です。
Failures due to other errors	他のエラーによる故障の数です。
Packets out of sequence	異なる順番のパケットによる故障の数です。
Packets arrived late	プローブがタイムアウトしたのち応答パケットを受信した数です。
UDP-jitter results	UDPジッタテストの結果です。このフィールドはUDPジッタテストのみ有効です。
Voice results	音声テストの結果です。このフィールドは音声テストのみ有効です。
RTT number	応答パケットを受信した数です。
Min positive SD	送信元から宛先への最小ポジティブジッタです。
Min positive DS	宛先から送信元への最小ポジティブジッタです。
Max positive SD	送信元から宛先への最大ポジティブジッタです。
Max positive DS	宛先から送信元への最大ポジティブジッタです。
Positive SD number	送信元から宛先へのポジティブジッタの数です。
Positive DS number	宛先から送信元へのポジティブジッタの数です。
Positive SD sum	送信元から宛先へのポジティブジッタの合計数です。
Positive DS sum	宛先から送信元へのポジティブジッタの合計数です。
Positive SD average	送信元から宛先への平均ポジティブジッタです。
Positive DS average	宛先から送信元への平均ポジティブジッタです。
Positive SD square-sum	送信元から宛先へのポジティブジッタの2乗和です。
Positive DS square-sum	宛先から送信元へのポジティブジッタの2乗和です。
Min negative SD	送信元から宛先へのネガティブジッタの絶対値の最小値です。

フィールド	説明
Min negative DS	宛先から送信元へのネガティブジッタの絶対値の最小値です。
Max negative SD	送信元から宛先へのネガティブジッタの絶対値の最大値です。
Max negative DS	宛先から送信元へのネガティブジッタの絶対値の最大値です。
Negative SD number	送信元から宛先へのネガティブジッタの数です。
Negative DS number	宛先から送信元へのネガティブジッタの数です。
Negative SD sum	送信元から宛先へのネガティブジッタの絶対値の合計です。
Negative DS sum	宛先から送信元へのネガティブジッタの絶対値の合計です。
Negative SD average	送信元から宛先へのネガティブジッタの絶対値の平均です。
Negative DS average	宛先から送信元へのネガティブジッタの絶対値の平均です。
Negative SD square-sum	送信元から宛先へのネガティブジッタの2乗和です。
Negative DS square-sum	宛先から送信元へのネガティブジッタの2乗和です。
One way results	片方向遅延です。 このフィールドはUDPジッタテスト、音声テストで有効です。
Max SD delay	送信元から宛先への最大遅延です。
Max DS delay	宛先から送信元への最大遅延です。
Min SD delay	送信元から宛先への最小遅延です。
Min DS delay	宛先から送信元への最小遅延です。
Number of SD delay	送信元から宛先への遅延の数です。
Number of DS delay	宛先から送信元への遅延の数です。
Sum of SD delay	送信元から宛先への遅延の合計です。
Sum of DS delay	宛先から送信元への遅延の合計です。
Square-Sum of SD delay	送信元から宛先への遅延の2乗和です。
Square-Sum of DS delay	宛先から送信元への遅延の2乗和です。

フィールド	説明
SD lost packets	送信元から宛先への損失したパケット数です。
DS lost packets	宛先から送信元への損失したパケット数です。
Lost packets for unknown reason	不明な理由で損失したパケット数です。
Voice scores	音声パラメータです。 このフィールドは音声テストで有効です。
Max MOS value	最大MOS値です。
Min MOS value	最小MOS値です。
Max ICPIF value	最大ICPIF値です。
Min ICPIF value	最小ICPIF値です。
Reaction statistics	カウント期間中のリアクションエントリに関する統計情報です。
Index	リアクションエントリのIDです。
Checked Element	モニタリングされる要素です。
Threshold Type	しきい値タイプです。
Checked Num	データ収集用にモニタリングされているターゲット数です。
Over-threshold Num	しきい値違反の数です。
Path	パスジッタテストでのパスのシリアル番号です。 このフィールドは、パスジッタテストでのみ使用できます。
Hop IP	ホップのIPアドレスです。 このフィールドは、パスジッタテストでのみ使用できます。
Path-jitter results	パスジッタのテスト結果です。 このフィールドは、パスジッタテストでのみ使用できます。
Jitter number	ジッタの数です。 このフィールドは、パスジッタテストでのみ使用できます。
Min/Max/Average jitter	最小/最大/平均の正のジッタです。単位はミリ秒です。 このフィールドは、パスジッタテストでのみ使用できます。

フィールド	説明
Positive jitter number	正のジッタの数です。 このフィールドは、パスジッタテストでのみ使用できます。
Min/Max/Average positive jitter	最小/最大/平均の正のジッタです。単位はミリ秒です。 このフィールドは、パスジッタテストでのみ使用できます。
Sum/Square-Sum positive jitter	正のジッタの合計/2乗和です。 このフィールドは、パスジッタテストでのみ使用できます。
Negative jitter number	負のジッタの数です。 このフィールドは、パスジッタテストでのみ使用できます。
Min/Max/Average negative jitter	最小/最大/平均の負のジッタです。単位はミリ秒です。 このフィールドは、パスジッタテストでのみ使用できます。
Sum/Square-Sum negative jitter	負のジッタの合計/2乗和です。 このフィールドは、パスジッタテストでのみ使用できます。

表 3-5 にしきい値モニタリングフィールドの説明を示します。

表 3-5 しきい値モニタリングフィールドの説明

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
probe-duration	accumulate	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
	average	ー	ー	ー
	consecutive	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
probe-fail	accumulate	カウント期間のプローブ	完了したプローブ数	プローブ失敗数
	consecutive	カウント期間のプローブ	完了したプローブ数	プローブ失敗数
RTT	accumulate	カウント期間のプローブ	送信したパケット数	ラウンドトリップ中にしきい値を超過したパケット数

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
	average	ー	ー	ー
jitter-DS/jitter-SD	accumulate	カウント期間のプローブ	送信したパケット数	1方向ジッタ時間中にしきい値を超過したパケット数
	average	ー	ー	ー
OWD-DS/OWD-SD	ー	カウント期間のプローブ	送信したパケット数	1方向ジッタ時間中にしきい値を超過したパケット数
packet-loss	accumulate	カウント期間のプローブ	送信したパケット数	パケット損失数
ICPIF/MOS (available only for the voice operation)	ー	ー	ー	ー

関連コマンド

statistics interval

3.1.11 filename

Syntax

filename *filename*

undo filename

デフォルト

設定なし

View

FTP operation view

FTP template view

定義済みユーザロール

network-admin

パラメータ

filename: FTP サーバと FTP クライアント間で転送するファイル名を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。スラッシュ（/）は含むことができません。

説明

filename コマンドは FTP サーバと FTP クライアント間で転送するファイル名を指定します。

undo filename コマンドはデフォルトに戻します。

例

FTP テストで、FTP サーバと FTP クライアント間で転送するファイル名を **config.txt** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] filename config.txt

FTP テンプレート view で、FTP サーバと FTP クライアント間で転送するファイル名を **config.txt** に設定します。

<Switch> system-view

[Switch] nqa template ftp ftptplt

[Switch-nqatplt-ftp-ftptplt] filename config.txt

3.1.12 frequency

Syntax

frequency *interval*

undo frequency

デフォルト

2 つの連続する音声テスト間隔は 60000 ミリ秒です。他のテストの 2 つの連続するテスト間隔は 0 ミリ秒です。

NQA テンプレート view では、連続する二つのテストの間隔は 5000 ミリ秒です。

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

すべての NQA template view

定義済みユーザロール

network-admin

パラメータ

interval: 2 つの連続するテスト間隔を指定します。設定範囲は 0〜604800000 ミリ秒です。0 を指定した場合、テストは 1 回だけ実行され、統計情報は作成しません。

説明

frequency コマンドは NQA テストを繰り返す間隔を設定します。

undo frequency コマンドはデフォルトに戻します。

テスト間隔になってもテストが完了しないとき、次のテストが開始します。

例

ICMP エコーテストを 1000 ミリ秒ごとに繰り返すように設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] frequency 1000

DNS テンプレート view で、1000 ミリ秒ごとに繰り返すように DNS テストを設定します。

<Switch> system-view

[Switch] nqa template dns dnstplt

[Switch-nqatplt-dns-dnstplt] frequency 1000

3.1.13 history-record enable

Syntax

history-record enable

undo history-record enable

デフォルト

履歴記録の保存は、UDP tracert テストに対してのみ有効です。

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

定義済みユーザロール

network-admin

説明

history-record enable コマンドは NQA テストの履歴記録を保存することを有効にします。

undo history-record enable コマンドは NQA テストの履歴記録を保存することを無効にします。

NQA テストの履歴記録を表示する場合、**display nqa history** コマンドを使用します。

undo history-record enable コマンドは NQA テストの既存の履歴記録も削除します。

例

NQA テストの履歴記録を保存することを有効にします。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] history-record enable

関連コマンド

display nqa history

3.1.14 history-record keep-time

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

デフォルト

120 分

View

CMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

定義済みユーザロール

network-admin

パラメータ

keep-time: 履歴記録を保存する期間を指定します。設定範囲は 1～1440 分です。

説明

history-record keep-time コマンドは NQA テストの履歴記録の有効期限を指定します。

undo history-record keep-time コマンドはデフォルトに戻します。

NQA テストが完了したとき、タイマが開始します。すべての記録は有効期限になったとき、削除されます。

例

ICMP エコーテストの履歴記録の有効期限を 100 分に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] history-record keep-time 100

3.1.15 history-record number

Syntax

history-record number *number*

undo history-record number

デフォルト

50

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

定義済みユーザロール

network-admin

パラメータ

number: NQA テストで履歴記録を保存できる最大数を指定します。設定範囲は 0～50 です。

説明

history-record number コマンドは NQA テストで履歴記録を保存できる最大数を設定します。

undo history-record number コマンドはデフォルトに戻します。

NQA テストの履歴記録の数が最大数を超過した場合、もっとも古い履歴記録が削除されます。

例

ICMP エコーテストで履歴記録を保存できる最大数を 10 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] history-record number 10

3.1.16 next-hop

Syntax

next-hop ip *ip-address*

undo next-hop ip

デフォルト

設定なし

View

ICMP echo operation view

定義済みユーザロール

network-admin

パラメータ

ip-address: ネクストホップ IPv4 アドレスを指定します。

説明

next-hop ip コマンドはプローブパケットのネクストホップ IPv4 アドレスを指定します。

undo next-hop ip コマンドは設定をデフォルトに戻します。

ネクストホップ IPv4 アドレスが設定されていない場合、装置はルーティングテーブルを検索し、プローブパケットのネクストホップ IPv4 アドレスを決定します。

例

ICMP エコーテストのネクストホップ IPv4 アドレスとして 10.1.1.1 を指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.1

3.1.17 nqa

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

all: すべての NQA テストを削除します。

説明

nqa コマンドは NQA テストを作成し、その view に移行します。

undo nqa コマンドはテストを削除します。

例

管理者 **admin** とテストタグ **test** の NQA テストを作成し、NQA operation view に移行します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test]

3.1.18 nqa agent enable

Syntax

nqa agent enable

undo nqa agent enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

nqa agent enable コマンドは NQA クライアントを有効にします。

undo nqa agent enable コマンドは NQA クライアントを無効にし、すべてのテストを停止します。

例

NQA クライアントを有効にします。

<Switch> system-view

[Switch] nqa agent enable

関連コマンド

nqa server enable

3.1.19 nqa schedule

Syntax

nqa schedule *admin-name operation-tag* **start-time** { *hh:mm:ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

undo nqa schedule *admin-name operation-tag*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

start-time: NQA テストの開始日時を指定します。

hh:mm:ss: NQA テストの開始時間を指定します。

yyyy/mm/dd: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

mm/dd/yyyy: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

now: すぐにテストを開始します。

lifetime: テストの有効期限を指定します。

lifetime: テスト期間を指定します。設定範囲は 1～2147483647 秒です。

forever: **undo nqa schedule** コマンドを使用して手動で停止するまでテストを実行します。

recurring: 開始時間に自動でテストを開始し、指定した期間、実行し続けます。このキーワードを指定しない場合、NQA テストは指定した日時に 1 回だけ実行されます。

説明

nqa schedule コマンドは NQA テストのスケジューリングのパラメータを設定します。

undo nqa schedule コマンドはテストを停止します。

NQA 工程は、指定した開始時間と終了時間(開始時間+テスト時間)の間に実行されます。指定した開始時刻がシステム時刻より前の場合、テストはただちに開始されます。指定した開始時刻と終了時刻の両方がシステム時刻より前の場合、テストは開始されません。現在のシステム時刻を表示するには、**display clock** コマンドを使用します。

スケジュールされた NQA テストの operation view あるいは operation type view に移行することはできません。移行する場合は、**undo nqa schedule** コマンドを使用して、最初に NQA テストを停止します。

テストを完了させるため、十分長い有効期限を指定してください。

例

管理者 **admin** とテストタグ **test** の NQA テストをスケジューリングし、2008 年 8 月 8 日の 08 時 08 分 08 秒に開始し、1000 秒間テストを行うように設定します。

<Switch> system-view

[Switch] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000 recurring

関連コマンド

- **destination ip**
- **display clock** (コマンドマニュアルのセクション 1 *はじめに*)
- **nqa**
- **type**

3.1.20 operation (FTP operation view)

Syntax

operation { **get** | **put** }

undo operation

デフォルト

get

View

FTP operation view

FTP template view

定義済みユーザロール

network-admin

パラメータ

get: FTP サーバからファイルを取得します。

put: FTP サーバにファイルを転送します。

説明

operation コマンドは FTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

filename コマンドで **put** オペレーションを実行するとき、NQA クライアント上にファイルが存在していることを確認してください。

FTP サーバからファイルを取得する場合、FTP サーバの URL に指定されたファイルが存在していることを確認してください。NQA クライアントは FTP サーバから取得したファイルを保存しません。

FTP テストではファイルサイズが小さいファイルを使用してください。大きいサイズのファイルは、タイムアウトでテストが失敗したり、ネットワークの帯域幅以上を独占して他のサービスに影響を与えたりする可能性があります。

例

FTP テストのオペレーションタイプを **put** に指定します。

FTP テストのテスト

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] operation put

FTP テンプレート view で、FTP テストのオペレーションタイプを **put** に指定します。

<Switch> system-view

[Switch] nqa template ftp ftptplt

[Switch-nqatplt-ftp-ftptplt] operation put

関連コマンド

- **password**
- **username**

3.1.21 operation (HTTP operation view/HTTPS template view)

Syntax

operation { **get** | **post** | **raw** }

undo operation

デフォルト

get

View

HTTP operation view

HTTPS operation view

HTTPS template view

定義済みユーザロール

network-admin

パラメータ

get: HTTP サーバあるいは HTTPS サーバからファイルを取得します。

post: HTTP サーバあるいは HTTPS サーバにファイルを転送します。

raw: RAW 要求を HTTP あるいは HTTPS サーバに送信します。

説明

operation コマンドは HTTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

HTTP あるいは HTTPS テストでは、HTTP あるいは HTTPS 要求をプローブパケットとして使用します。

HTTP の **get** あるいは **post** オペレーションの HTTP 要求の内容は **url** コマンドによって指定された URL から取得されます。

例

HTTP テストのオペレーションのタイプを **raw** に指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type http

[Switch-nqa-admin-test-http] operation raw

HTTP テンプレート view で、HTTP テストのオペレーションのタイプを **raw** に設定します。

<Switch> system-view

[Switch] nqa template http httptplt

[Switch-nqatplt-http-httptplt] operation raw

関連コマンド

- **password**
- **username**

3.1.22 password

Syntax

password { **cipher** | **simple** } *string*

undo password

デフォルト

設定なし

View

FTP/HTTP operation view

FTP/HTTP/HTTPS/RADIUS template view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号パスワードを指定します。

simple: プレーンパスワードを指定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは暗号テキストで保存されます。

string: パスワードを指定します。値は以下のように変わります。

- FTP、HTTP、および HTTPS テストの場合、プレーンテキストのパスワードは、大文字、小文字を区別します。設定範囲は 1～32 文字です。パスワードの暗号化形式は、大文字、小文字を区別します。設定範囲は、1～73 文字です。
- RADIUS テンプレートの場合、パスワードのプレーンテキストは、大文字、小文字を区別します。設定範囲は 1～64 文字です。パスワードの暗号化形式は、大文字小文字を区別します。設定範囲は 1～117 文字です。

説明

password コマンドはパスワードを設定します。

undo password コマンドは設定をデフォルトに戻します。

例

FTP ログインパスワードを **ftpuser** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] password simple ftpuser

FTP テンプレート view で FTP ログインパスワードを **ftpuser** に設定します。

<Switch> system-view

[Switch] nqa template ftp ftptplt

[Switch-nqatplt-ftp-ftptplt] password simple ftpuser

関連コマンド

- **operation**

- **username**

3.1.23 probe count

Syntax

probe count *times*

undo probe count

デフォルト

UDP tracert テストでは、NQA クライアントはパス上の各ホップに 3 つのプローブパケットを送信します。

その他のタイプのテストでは、NQA クライアントはテストごとに 1 つのプローブを宛先に対して実行します。

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

times: プローブの時間を指定します。

- UDP tracert テストの場合、パス上の各ホップに対する検証の回数を指定します。設定範囲は 1～10 です。
- その他のタイプのテストでは、テストごとのターゲットに対するプローブの回数を指定します。設定範囲は 1～15 です。

説明

probe count コマンドは NQA テストの検査回数を設定します。

undo probe count コマンドはデフォルトに戻します。

以下に異なるタイプのテストを実行する方法を示します。

- TCP あるいは DLSw テストは接続を設定します。
- ICMP ジッタあるいは UDP ジッタは多くのプローブパケットを送信します。多くのプローブパケットは **probe packet-number** コマンドによって設定されます。
- FTP テストはファイルをアップロードあるいはダウンロードします。
- HTTP テストは Web ページを取得します。

- DHCP テストは DHCP を介して IP アドレスを取得します。
- DNS テストはドメイン名を IP アドレスに変換します。
- ICMP エコーテストは ICMP エコー要求を送信します。
- UDP エコーテストは UDP パケットを送信します。
- SNMP テストは 1 つの SNMPv1 パケット、1 つの SNMPv2c パケット、1 つの SNMPv3 パケットを送信します。
- UDP tracert テストは、ソースから宛先へのルーティングパスを決定します。各ホップに送信されるプローブパケットの数は、**probe count** コマンドを使用して設定されます。
- フレーム損失、遅延、またはスループットテストは、プローブフレームを宛先装置に送信して、ネットワークのフレーム損失率、遅延、またはスループットをテストします。

テストが複数のプローブを実行する場合、NQA クライアントは以下の状況で新しいプローブを開始します。

- NQA クライアントが最後のプローブで送信したパケットの応答を受信します。
- プローブのタイムアウト時間が終了します。

このコマンドは音声、音声あるいはパスジッタテストでは無効です。これらのテストは 1 つのプローブのみ実行します。

例

ICMP エコーテストを実行する検査回数を 10 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] probe count 10

3.1.24 probe packet-interval

Syntax

probe packet-interval *packet-number*

undo probe packet-interval

デフォルト

20 ミリ秒

View

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

packet-interval: パケットを送信する間隔を指定します。設定範囲は 10～60000 ミリ秒です。

説明

probe packet-interval コマンドはプローブのパケット送信間隔を設定します。

undo probe packet-interval コマンドはデフォルトに戻します。

例

UDP ジッタテストのパケット送信間隔を 100 ミリ秒に設定します。

<AC> system-view

[AC] nqa entry admin test

[AC-nqa-admin-test] type udp-jitter

[AC-nqa-admin-test-udp-jitter] probe packet-interval 100

3.1.25 probe packet-number

Syntax

probe packet-number *packet-number*

undo probe packet-number

デフォルト

ICMP ジッタ、UDP ジッタ、あるいはパスジッタのプローブは 10 パケットを送信し、音声プローブは 1000 パケットを送信します。

View

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

packet-number: プローブごとに送信するパケット数を指定します。使用可能な値の範囲は以下のとおりです。

- ICMP ジッタ、UDP ジッタ、およびパスジッタテストの設定範囲は 10～1000 です。
- 音声テストの設定範囲は 10～60000 です。

説明

probe packet-number コマンドは UDP ジッタテスト、パスジッタテスト、音声テストで送信するパケットの数を設定します。

undo probe packet-number コマンドはデフォルトに戻します。

例

UDP ジッタテストで 100 パケットを送信するように設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type udp-jitter

[Switch-nqa-admin-test-udp-jitter] probe packet-number 100

3.1.26 probe packet-timeout

Syntax

probe packet-timeout *timeout*

undo probe packet-timeout

デフォルト

UDP ジッタテストあるいはパスジッタテストの応答タイムアウト時間は 3000 ミリ秒です。

音声テストの応答タイムアウト時間は 5000 ミリ秒です。

View

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

timeout: タイムアウト時間を指定します。単位はミリ秒です。設定範囲は 10～3600000 ミリ秒です。

説明

probe packet-timeout コマンドは UDP ジッタテスト、パスジッタテスト、音声テストの応答を待つタイムアウト時間を設定します。

undo probe packet-timeout コマンドはデフォルトに戻します。

例

UDP ジッタテストの応答を待つタイムアウト時間を 100 ミリ秒に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type udp-jitter

[Switch-nqa-admin-test-udp-jitter] probe packet-timeout 100

3.1.27 probe timeout

Syntax

probe timeout *timeout*

undo probe timeout

デフォルト

3000 ミリ秒

View

FTP/HTTP/SNMP/TCP operation view

ICMP/UDP echo operation view

定義済みユーザロール

network-admin

パラメータ

timeout: プローブのタイムアウト時間を指定します。単位はミリ秒です。

- FTP テスト、HTTP テストの設定範囲は 10～86400000 ミリ秒です。
- DHCP テスト、ICMP エコーテスト、SNMP テスト、TCP テスト、UDP エコーテストあるいは UDP tracert テストの設定範囲は 10～3600000 ミリ秒です。
- FTP、HTTP、あるいは HTTPS テンプレートの設定範囲は 10～86400000 ミリ秒です。
- その他のタイプの NQA テンプレートの設定範囲は 10～3600000 ミリ秒です。

説明

probe timeout コマンドはプローブのタイムアウト時間を設定します。

undo probe timeout コマンドはデフォルトに戻します。

プローブの時間以内にテストが完了しない場合、プローブがタイムアウトします。

例

DHCP テストのプローブタイムアウト時間を 10000 ミリ秒に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type dhcp

[Switch-nqa-admin-test-dhcp] probe timeout 10000

HTTP テンプレート view で、HTTP テストのプローブタイムアウト時間を 10000 ミリ秒に設定します。

<Switch> system-view

[Switch] nqa template http httptplt

[Switch-nqatplt-http-httptplt] probe timeout 10000

3.1.28 reaction checked-element probe-fail (for trap)

Syntax

reaction *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

定義済みユーザロール

network-admin

パラメータ

item-number: リアクションエントリに ID を割り当てます。設定範囲は 1～10 です。

threshold-type: しきい値タイプを指定します。

accumulate *accumulate-occurrences*: プローブが失敗する総数を確認します。設定範囲は 1～15 です。

consecutive *consecutive-occurrences*: 連続してテストに失敗する最大数を指定します。設定範囲は 1～16 です。

action-type: トリガとなるアクションを指定します。デフォルトのアクションは **none** です。

none: ターミナル端末に結果を表示します。

trap-only: ターミナル端末に結果を表示し、NMS に SNMP トラップメッセージを送信します。DNS テストでは無効です。

説明

reaction checked-element probe-fail コマンドはテストのプローブの失敗をモニタするためのリアクションエントリを設定します。

undo reaction コマンドは指定されたリアクションエントリを削除します。

リアクションを作成した後、修正することはできません。リアクションエントリの属性を変更する場合、**undo reaction** コマンドを使用して最初にエントリを削除し、新しいリアクションエントリを再度設定してください。

例

ICMP エコーテストのプローブ失敗をモニタするため、リアクションエントリ 1 を作成します。NQA テストを開始する前に、リアクションエントリの初期状態は無効です。プローブが失敗した回数が 10 以上になった場合、エントリの状態をしきい値超過に設定します。しきい値が下回った場合、エントリの状態をしきい値以下に設定します。一度リアクションエントリの状態が変更するとトラップメッセージを作成し、NMS に送信します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type accumulate 10 action-type trap-only

ICMP エコーテストのプローブ失敗をモニタするため、リアクションエントリ 2 を作成します。NQA テストを開始する前に、リアクションエントリの初期状態は無効です。連続してプローブが失敗した回数が 10 以上になった場合、エントリの状態をしきい値超過に設定します。しきい値が下回った場合、エントリの状態をしきい値以下に設定します。一度リアクションエントリの状態が変更するとトラップメッセージを作成し、NMS に送信します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-fail threshold-type consecutive 10 action-type trap-only

3.1.29 reaction trap

Syntax

reaction trap { **path-change** | **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }

undo reaction trap { **path-change** | **probe-failure** | **test-complete** | **test-failure** }

デフォルト

設定なし

View

DHCP/DLSw/DNS/FTP/HTTP/SNMP/TCP/voice operation view

ICMP/UDP echo operation view

UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

path-change: UDP tracert テストによって宛先への別のパスが検出された場合にトラップを送信します。

probe-failure *consecutive-probe-failures*: 連続してテストが失敗した後、NMS にトラップを送信するよう設定します。*consecutive-probe-failures* はテストにおける連続失敗数を設定します。設定範囲は 1～15 です。システムは複数のトラップを送信できるように各テストで連続して失敗した回数をカウントします。

test-complete: テストが完了したことを通知するためにトラップを送信します。

test-failure: プローブの失敗回数の総数が *cumulate-probe-failures* 以上になった場合、トラップを送信します。設定範囲は 1～15 です。システムは、1 つのトラップのみ送信するため、最後にテストを完了した後、プローブが失敗した総数をカウントします。

accumulate-probe-failures: テストで失敗したプローブの総数を指定します。設定範囲は 1～15 です。UDP tracert テストではサポートされていません。

説明

reaction trap コマンドは指定した状況下で NMS にトラップを送信するように設定します。

undo reaction trap コマンドはデフォルトに戻します。

reaction trap test-complete コマンドは ICMP ジッタテスト、UDP ジッタテスト、音声テストでのみ有効です。

UDP tracert テストでは、次のパラメータは使用できません。

- **probe-failure** *continuative-probe-failures* オプション
- *accumulate-probe-failures*

例

ICMP エコーテストで連続して 5 回以上失敗した場合、トラップを送信するように設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] reaction trap probe-failure 5

3.1.30 resolve-target

Syntax

resolve-target *domain-name*

undo resolve-target

デフォルト

設定なし

View

DNS operation view

DNS template view

定義済みユーザロール

network-admin

パラメータ

domain-name: 解決されるドメイン名を指定します。設定範囲は 1～255 文字です。ドットで区切り、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます（たとえば、aabbcc.com です）。各部分の設定範囲は 1～63 文字です。連続したドット（.）は使用できません。

説明

resolve-target コマンドは DNS テストのドメイン名を設定します。

undo resolve-target コマンドはデフォルトに戻します。

例

解決されるドメイン名 **domain1** を設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type dns

[Switch-nqa-admin-test-dns] resolve-target domain1

DNS テンプレート view で、解決するドメイン名として **domain1** を指定します。

<Switch> system-view

[Switch] nqa template dns dnstplt

[Switch-nqatplt-dns-dnstplt] resolve-target domain1

3.1.31 route-option bypass-route

Syntax

route-option bypass-route

undo route-option bypass-route

デフォルト

無効

View

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/voice operation view

定義済みユーザロール

network-admin

説明

route-option bypass-route コマンドはダイレクトな宛先への接続性を確認するため、ルーティングテーブルバイパス機能を有効にします。

undo route-option bypass-route コマンドはルーティングバイパス機能を無効にします。

ルーティングテーブルバイパス機能が有効であるとき、以下のイベントが発生します。

- ルーティングテーブルは検索されません。パケットは、直接接続されたネットワーク上の宛先に送信されます。
- プローブパケットの TTL 値は 1 に設定されます。**ttl** コマンドで設定された TTL は有効になりません。

このコマンドは、NQA テストの宛先アドレスが IPv6 アドレスの場合は有効になりません。

例

ルーティングテーブルバイパス機能を有効にします。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] route-option bypass-route

3.1.32 source interface (ICMP echo/UDP tracert operation view)

Syntax

source interface *interface-type interface-number*

undo source interface

デフォルト

ICMP エコー要求パケットは送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

ICMP echo operation view

UDP tracert operation view

ICMP template view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

source interface コマンドは ICMP エコー要求パケットの送信元 IP アドレスとして指定したインタフェースの IP アドレスを指定します。

undo source interface コマンドはデフォルトに戻します。

指定されたインタフェースは起動している必要があります。インタフェースがダウンしていると、プローブ要求を送信できません。

ICMP エコーテストまたは ICMP テンプレートに対して、**source ip** コマンドあるいは **source ipv6** コマンドと **source interface** コマンドの両方を設定した場合、最後に行った設定が適用されます。

source interface コマンドと **source ip** コマンドを UDP tracert テストに対して複数回実行すると、最後に行った設定が適用されます。

例

ICMP エコー要求パケットの送信元 IP アドレスとして VLAN インタフェース 1 の IP アドレスを設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] source interface vlan-interface 1

ICMP テンプレート view で、ICMP エコー要求パケットの送信元 IP アドレスとして VLAN インタフェース 1 の IP アドレスを設定します。

<Switch> system-view

[Switch] nqa template icmp icmptplt

[Switch-nqatplt-icmp-icmptplt] source interface vlan-interface 1

関連コマンド

source ip

3.1.33 source ip

Syntax

source ip *ip-address*

undo source ip

デフォルト

プローブパケットは、出力インタフェースのプライマリ IP アドレスを送信元 IP アドレスとして使用します。

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Any NQA template view

定義済みユーザロール

network-admin

パラメータ

ip-address: プローブパケットの送信元 IPv4 アドレスを指定します。

説明

source ip コマンドはプローブパケットの送信元 IPv4 アドレスを設定します。

undo source ip コマンドは設定をデフォルトに戻します。

指定する送信元 IPv4 アドレスは、ローカルインタフェースの IPv4 アドレスである必要があり、ローカルインタフェースは稼働している必要があります。そうしないと、プローブパケットを送信できません。

NQA テンプレートの場合、送信元アドレスと宛先アドレスの IP バージョンが異なると、送信元アドレスは有効になりません。

ICMP エコーテスト、ICMP テンプレート、または UDP tracert テストのために **source interface** コマンドと **source ip** コマンドを複数回実行すると、最新の設定が有効になります。

例

ICMP エコー要求の送信元 IPv4 アドレスを 10.1.1.1 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] source ip 10.1.1.1

ICMP テンプレート view で、ICMP エコー要求の送信元 IPv4 アドレスを 10.1.1.1 に設定します。

<Switch> system-view

[Switch] nqa template icmp icmptplt

[Switch-nqatplt-icmp-icmptplt] source ip 10.1.1.1

関連コマンド

source interface

3.1.34 source port

Syntax

source port *port-number*

undo source port

デフォルト

設定なし

View

UDP echo operation view

SNMP operation view

UDP tracert operation view

UDP jitter/voice operation view

DNS template view

定義済みユーザロール

network-admin

パラメータ

port-number: 送信元ポート番号を指定します。設定範囲は 1～65535 です。

説明

source port コマンドはプローブパケットの送信元ポートを設定します。

undo source port コマンドはデフォルトに戻します。

例

UDP エコーテストのプローブパケットで送信元ポートを 8000 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type udp-echo

[Switch-nqa-admin-test-udp-echo] source port 8000

DNS テンプレート view で、DNS テストのプローブパケットで送信元ポート番号を 8000 に設定します。

<Switch> system-view

[Switch] nqa template dns dnstplt

[Switch-nqatplt-dns-dnstplt] source port 8000

3.1.35 statistics interval

Syntax

statistics interval *interval*

undo statistics interval

デフォルト

60 分

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

interval: 統計情報を収集する間隔を指定します。設定範囲は 1～35791394 分です。

説明

statistics interval コマンドは NQA テストで統計情報を収集する間隔を設定します。

undo statistics interval コマンドはデフォルトに戻します。

NQA は指定した間隔で NQA テストを行い、テスト結果の統計情報を計算します。これらの統計は統計グループを作ります。統計情報グループの情報を表示する場合、**display nqa statistics** コマンドを使用します。

例

ICMP エコーテストで統計情報を収集する間隔を 2 分に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] statistics interval 2

3.1.36 statistics max-group

Syntax

statistics max-group *number*

undo statistics max-group

デフォルト

最大で 2 つの統計情報グループを登録できます。

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

number: 統計情報グループの最大数を指定します。設定範囲は 0～100 です。統計情報の収集を無効にする場合、0 に設定します。

説明

statistics max-group コマンドは保存できる統計情報グループの最大数を設定します。

undo statistics max-group コマンドはデフォルトに戻します。

統計情報グループの数が最大数に到達し、新しいグループが保存されたとき、もっとも古い統計情報が削除されます。

例

ICMP テストで保存できる統計情報グループの最大数を 5 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] statistics max-group 5

3.1.37 tos

Syntax

tos *value*

undo tos

デフォルト

0

View

すべての operation view

すべての NQA template view

定義済みユーザロール

network-admin

パラメータ

value: ToS を指定します。設定範囲は 0～255 です。

説明

tos コマンドはプローブパケットの IP ヘッダの ToS を設定します。

undo tos コマンドはデフォルトに戻します。

例

ICMP エコーテスト view で、プローブパケットの IP ヘッダの ToS を 1 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] tos 1

ICMP テンプレート view で、プローブパケットの IP ヘッダの ToS を 1 に設定します。

<Switch> system-view

[Switch] nqa template icmp icmptplt

[Switch-nqatplt-icmp-icmptplt] tos 1

3.1.38 ttl

Syntax

ttl *value*

undo ttl

デフォルト

ホップの最大数は、UDP tracert テストのプローブパケットは 30、その他の種類のテストのプローブパケットは 20 です。

View

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/voice operation view

Any NQA template view

定義済みユーザロール

network-admin

パラメータ

value: プローブパケットの TTL を指定します。設定範囲は 1～255 です。

説明

ttl コマンドはプローブパケットが通過できるホップの最大数を設定します。

undo ttl コマンドはデフォルトに戻します。

route-option bypass-route コマンドはプローブパケットの TTL を 1 に設定します。あるテストに対して **route-option bypass-route** コマンドと ttl コマンドの両方を設定した場合、ttl コマンドは有効になりません。

UDP tracert テストが成功した場合は、最大ホップ数が **init-ttl** コマンドに設定された値より小さくないことを確認します。

例

ICMP エコーテストで、プローブパケットの最大ホップ数を 16 に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type icmp-echo

[Switch-nqa-admin-test-icmp-echo] ttl 16

ICMP テンプレート view で、プローブパケットの最大ホップ数を 16 に設定します。

<Switch> system-view

[Switch] nqa template icmp icmptplt

[Switch-nqatplt-icmp-icmptplt] ttl 16

3.1.39 type

Syntax

type { **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **icmp-jitter** | **path-jitter** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** | **udp-tracert** | **voice** }

デフォルト

設定なし

View

NQA operation view

定義済みユーザロール

network-admin

パラメータ

dhcp: DHCP テストタイプを指定します。

dlsw: DLSw テストタイプを指定します。

dns: DNS テストタイプを指定します。

ftp: FTP テストタイプを指定します。

http: HTTP テストタイプを指定します。

icmp-echo: ICMP エコーテストタイプを指定します。

icmp-jitter: ICMP ジッタテストタイプを指定します。

path-jitter: パスジッタテストタイプを指定します。

snmp: SNMP テストタイプを指定します。

tcp: TCP テストタイプを指定します。

udp-echo: UDP エコーテストタイプを指定します。

udp-jitter: UDP ジッタテストタイプを指定します。

udp-tracert: UDP tracert テストタイプを指定します。

voice: 音声テストタイプを指定します。

説明

type コマンドは NQA テストのテストタイプを設定し、operation type view に移行します。

NQA 工程に指定できるタイプは 1 つのみです。その後、NQA テストのテストタイプを設定できます。NQA 工程のタイプを変更するには、system view で NQA 工程を削除し、NQA 工程を再作成します。

例

NQA テストタイプとして FTP を選択し、FTP operation view に移行します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp]

3.1.40 url

Syntax

url *url*

undo url

デフォルト

設定なし

View

FTP/HTTP operation view

FTP/HTTP/HTTPS template view

定義済みユーザロール

network-admin

パラメータ

url: 宛先サーバの URL を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。以下の表に異なるテストの URL のフォーマットとパラメータを示します。

表 3-6 URL のフォーマットとパラメータ

テスト	URL フォーマット	パラメータの説明
HTTPテスト	*http://host/resource* *http://host:port/resource*	hostパラメータの設定範囲は1～255文字です。ドットで区切られ、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます。たとえばaabbcc.comです。各部分の設定範囲は1～63文字です。連続してドット（.）疑問符は設定することができません。ファイル名のパラメータの詳細は、QX-W2300ACシリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*10章 ファイルシステム管理*”を参照してください。
HTTPSテスト	*https://host/resource* *https://host:port/resource*	
FTPテスト	*ftp://host/filename* *ftp://host:port/filename*	

説明

url コマンドは宛先 URL を指定します。

undo url コマンドは URL を削除します。

例

HTTP テストの URL を **http://www.company.com/index.htm** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type http

[Switch-nqa-admin-test-http] url http://www.company.com/index.html

HTTP テンプレート view で、HTTP テストの URL を **http://www.company.com/index.htm** に設定します。

<Switch> system-view

[Switch] nqa template http httptplt

[Switch-nqatplt-http-httptplt] url http://www.company.com/index.html

3.1.41 username

Syntax

username *username*

undo username

デフォルト

設定なし

View

FTP/HTTP operation view

FTP/HTTP/HTTPS/RADIUS template view

定義済みユーザロール

network-admin

パラメータ

username: ユーザ名を指定します。大文字、小文字を区別します。FTP、HTTP、または HTTPS ユーザ名の設定範囲は 1～32 文字です。RADIUS 認証ユーザ名の設定範囲は 1～253 文字の文字列です。

説明

username コマンドはユーザ名を指定します。

undo username コマンドはデフォルトに戻します。

例

FTP ログインのユーザ名を **administrator** に設定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type ftp

[Switch-nqa-admin-test-ftp] username administrator

FTP テンプレート view で、FTP ログインのユーザ名を **administrator** に設定します。

<Switch> system-view

[Switch] nqa template ftp ftptplt

[Switch-nqatplt-ftp-ftptplt] username administrator

関連コマンド

- **operation**
- **password**

3.1.42 Version (HTTP operation view, HTTP/HTTPS template view)

Syntax

version { **v1.0** | **v1.1** }

undo version

デフォルト

1.0

View

HTTP operation view

HTTP/HTTPS template view

定義済みユーザロール

network-admin

パラメータ

v1.0: HTTP バージョン 1.0 を使用します。

v1.1: HTTP バージョン 1.1 を使用します。

説明

version コマンドは HTTP テストあるいは HTTPS テストで使用する HTTP バージョンを指定します。

undo version コマンドはデフォルトに戻します。

例

HTTP テストで使用する HTTP バージョンを 1.1 に指定します。

<Switch> system-view

[Switch] nqa entry admin test

[Switch-nqa-admin-test] type http

[Switch-nqa-admin-test-http] version v1.1

3.2 NQAサーバ設定コマンド

注意:

UDP ジッタテスト、TCP テスト、UDP エコーテスト、音声テストを行うため、NQA サーバを設定します。

3.2.1 display nqa server

Syntax

display nqa server

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nqa server コマンドは NQA サーバの状態を表示します。

例

NQA サーバの状態を表示します。

<Switch> display nqa server

```
NQA server status: Enabled
TCP connect:
  IP address         Port     Tos    VPN instance
  2.2.2.2           2000     200    -
UDP echo:
  IP address         Port     Tos    VPN instance
  3.3.3.3           3000     255    -
```

表 3-7 コマンド出力

フィールド	説明
NQA server status	NQAサーバが有効かどうかです。
TCP connect	NQAサーバのTCPリスニングサービスの情報です。

フィールド	説明
UDP echo	NQAサーバのUDPリスニングサービスの情報です。
IP address	NQAサーバのTCP/UDPリスニングサービスで指定されたIPアドレスです。
Port	NQAサーバのTCP/UDPリスニングサービスでの指定されたポート番号です。
Tos	NQAサーバによって送信された応答パケットのToSの値です。
VPN instance	NQAサーバが受信するIPアドレスが属するVPNインスタンスの名前です。NQAサーバがパブリックIPアドレスを受信する場合、このフィールドにはハイフン(-)が表示されます。

関連コマンド

- **nqa server enable**
- **nqa server tcp-connect**
- **nqa server udp-echo**

3.2.2 nqa server enable

Syntax

nqa server enable

undo nqa server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nqa server enable コマンドは NQA サーバを有効にします。

undo nqa server enable コマンドは NQA サーバを無効にします。

例

NQA サーバを有効にします。

<Switch> system-view

[Switch] nqa server enable

関連コマンド

- **display nqa server**
- **nqa server tcp-connect**
- **nqa server udp-echo**

3.2.3 nqa server tcp-connect

Syntax

nqa server tcp-connect *ip-address port-number* [**tos** *tos*]

undo nqa server tcp-connect *ip-address port-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: TCP リスニングサービスの IP アドレスを指定します。

port-number: TCP リスニングサービスのポート番号を指定します。設定範囲は 1～65535 です。

vpn-instance *vpn-instance-name*: VPN インスタンスを名前で指定します。大文字、小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、NQA サーバはパブリック IP アドレスをリスニングします。

tos *tos*: 応答パケットの IP ヘッダの ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

nqa server tcp-connect コマンドは NQA サーバが指定された IP アドレスとポート番号をリスニングし、応答するため、TCP リスニングサービスを設定します。

undo nqa server tcp-connect コマンドは TCP リスニングサービスを削除します。

TCP テストだけのために NQA サーバでコマンドを設定する必要があります。

NQA サーバの TCP リスニングサービスの IP アドレスとポート番号を設定するとき、以下の制限とガイドラインに従ってください。

- IP アドレスとポート番号は NQA サーバで一意に設定し、NQA クライアントの設定に一致するようにしてください。
- IP アドレスは NQA サーバのインタフェースの IP アドレスにする必要があります。
- NQA テストを正常に実行し、既存のサービスへの影響を防ぐため、TCP リスニングサービスで 1～1023 の well-known ポートを設定しないでください。

例

NQA サーバで TCP リスニングサービスを設定し、IP アドレス 169.254.10.2、ポート番号 9000 をリスニングし、応答するように設定します。

<Switch> system-view

[Switch] nqa server tcp-connect 169.254.10.2 9000

関連コマンド

- **display nqa server**
- **nqa server enable**

3.2.4 nqa server udp-echo

Syntax

nqa server udp-echo *ip-address port-number* [**tos** *tos*]

undo nqa server udp-echo *ip-address port-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: UDP リスニングサービスの IP アドレスを指定します。

port-number: UDP リスニングサービスのポート番号を指定します。設定範囲は 1～65535 です。

vpn-instance *vpn-instance-name*: VPN インスタンスを名前で指定します。大文字小文字を区別し、設定範囲は 1～31 文字です。このオプションを指定しない場合、NQA サーバはパブリック IP アドレスをリスニングします。

tos *tos*: 応答パケットの IP ヘッダの ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

nqa server udp-echo コマンドは NQA サーバが指定された IP アドレスとポート番号をリスニングし、応答するため、UDP リスニングサービスを設定します。

undo nqa server udp-echo コマンドは UDP リスニングサービスを削除します。

UDP ジッタテスト、UDP エコーテスト、音声テストだけのために NQA サーバでコマンドを設定する必要があります。

NQA サーバの UDP リスニングサービスの IP アドレスとポート番号を設定するとき、以下の制限とガイドラインに従ってください。

- IP アドレスとポート番号は NQA サーバで一意に設定し、NQA クライアントの設定に一致するようにしてください。
- IP アドレスは NQA サーバのインタフェースの IP アドレスにする必要があります。
- NQA テストを正常に実行し、既存のサービスへの影響を防ぐため、UDP リスニングサービスで 1～1023 の well-known ポートを設定しないでください。

例

NQA サーバで UDP リスニングサービスを設定し、IP アドレス 169.254.10.2、ポート番号 9000 をリスニングし、応答するように設定します。

<Switch> system-view

[Switch] nqa server udp-echo 169.254.10.2 9000

関連コマンド

- **display nqa server**
- **nqa server enable**

目次

このセクションのページは **17-x-x** です。

4 章 SNMP 4-1
4.1 SNMP 設定コマンド 4-1
4.1.1 display snmp-agent community 4-1
4.1.2 display snmp-agent group 4-3
4.1.3 display snmp-agent local-engineid 4-5
4.1.4 display snmp-agent mib-view 4-5
4.1.5 display snmp-agent statistics 4-7
4.1.6 display snmp-agent sys-info 4-9
4.1.7 display snmp-agent trap queue 4-10
4.1.8 display snmp-agent trapbuffer drop 4-11
4.1.9 display snmp-agent trapbuffer send 4-11
4.1.10 display snmp-agent trap-list 4-12
4.1.11 display snmp-agent usm-user 4-13
4.1.12 enable snmp trap updown 4-15
4.1.13 reset snmp-agent trapbuffer 4-16
4.1.14 simulate snmp-trap 4-17
4.1.15 snmp-agent 4-19
4.1.16 snmp-agent { inform | trap } source 4-20
4.1.17 snmp-agent calculate-password 4-21
4.1.18 snmp-agent community 4-23
4.1.19 snmp-agent group 4-27
4.1.20 snmp-agent local-engineid 4-29
4.1.21 snmp-agent log 4-30
4.1.22 snmp-agent mib-view 4-31
4.1.23 snmp-agent packet max-size 4-32
4.1.24 snmp-agent packet response dscp 4-33
4.1.25 snmp-agent sys-info contact 4-34
4.1.26 snmp-agent sys-info location 4-35
4.1.27 snmp-agent sys-info version 4-36
4.1.28 snmp-agent target-host 4-37
4.1.29 snmp-agent trap enable 4-38
4.1.30 snmp-agent trap if-mib link extended 4-40
4.1.31 snmp-agent trap life 4-41
4.1.32 snmp-agent trap log 4-41
4.1.33 snmp-agent trap queue-size 4-42

4.1.34 snmp-agent usm-user { v1 | v2c } 4-43
4.1.35 snmp-agent usm-user v3 4-45

4章 SNMP

4.1 SNMP設定コマンド

SNMP エージェントはリンク状態の変更、ユーザのログイン、ログアウトのような重要なイベントを NMS に知らせるため、notification（トラップと inform）を送信します。特に指定しない限り、コマンドラインの trap キーワードは trap と inform を含みます。

4.1.1 display snmp-agent community

Syntax

display snmp-agent community [**read** |**write**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

read: 読み出し専用コミュニティ情報を表示します。

write: 読み出し、書き込みコミュニティ情報を表示します。

説明

display snmp-agent community コマンドは SNMPv1 または SNMPv2c のコミュニティ情報を表示します。

パラメータを指定しない場合は、すべての SNMP コミュニティの情報が表示されます。

ユーザがコミュニティを作成するには、次の 2 つの方法があります。

- snmp-agent community コマンドを使用してコミュニティを作成します。
- 設定 snmp-agent usm-user {v1|v2c}および snmp-agent group {v1|v2c}コマンド SNMPv1 または SNMPv2c ユーザと対応するグループが正常に作成されると、ユーザ名をコミュニティ名として使用するコミュニティが自動的に作成されます。

display snmp-agent community では、両方の方法で作成され、構成ファイルにクリアテキストで保存されたコミュニティの情報が表示されます。

例

#すべてのコミュニティ情報を表示します。

<Sysname> display snmp-agent community

```
Community name:aa
Group name:aa
ACL:2900
Storage-type:nonVolatile
Context name:con 1

Community name:bb
Role name:bb
Storage-type:nonVolatile

Community name:userv1
Group name:testv1
Storage-type:nonVolatile

Community name:cc
Group name:cc
ACL name:testacl
Storage-type:nonVolatile
```

表 4-1 コマンド出力

フィールド	説明
Community name	グループ名: ● コミュニティ名がsnmp-agent communityコマンドで作成された場合は、コミュニティ名が表示されます。 ● コミュニティ名がsnmp-agent usm-user {v 1|v 2 c}コマンドで作成された場合は、ユーザ名が表示されます。
Group name	グループ名: ● グループ名がsnmp-agent communityコマンドのVACMを使用して作成された場合、グループ名とグループ名は同じです。 ● コミュニティ名がsnmp-agent usm-user {v 1|v 2 c}コマンドで作成された場合は、ユーザのグループ名が表示されます。
Role name	コミュニティのユーザロールです。 コミュニティがRBACモードのsnmp-agent communityコマンドで作成された場合、ユーザロールはコミュニティ名と結合できます。
ACL	ACL番号です。 このフィールドはSNMPv1あるいはSNMPv2cコミュニティで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	使用するACLリストの名前(このフィールドは、コミュニティ名がACL名に指定されている場合にのみ表示されます。)
IPV6 ACL	使用されるIPv6 ACLリストの数(このフィールドは、コミュニティ名がIPv6 ACL番号にバインドされている場合にのみ表示されます。)

フィールド	説明
IPV6 ACL name	使用されているIPv6 ACLリストの名前(このフィールドは、コミュニティ名がIPv6 ACL名にバインドされている場合にのみ表示されます。)
Storage-type	記憶媒体のタイプです。 ● volatile:再起動後に情報が失われる ● nonVolatile–システムが再起動しても設定は失われません。 ● permanent—システムが再起動しても設定は失われません。変更することができますが、削除することができません。 ● readOnly—システムが再起動しても設定は失われません。変更あるいは削除することができません。 ● other—他の記憶媒体のタイプです。
Context name	SNMPの内容です。 ● SNMPコミュニティとSNMPの内容間のマッピングが設定されている場合、SNMPの内容が表示されます。 ● SNMPコミュニティとSNMPの内容間のマッピングが設定されていない場合、表示されません。

関連コマンド

- snmp-agent community
- snmp-agent usm-user {v1|v2}

4.1.2 display snmp-agent group

Syntax

display snmp-agent group [*group-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-name：情報を表示する SNMPv1、SNMPv2c、または SNMPv3 グループの名前を指定します。値の範囲は 1 ～ 32 文字の文字列で、大文字と小文字が区別されます。このパラメータが指定されていない場合、デバイスで作成されたすべての SNMP グループの情報が表示されます。

説明

display snmp-agent group コマンドは、SNMP グループ情報を表示します。

例

#すべての SNMP グループの情報を表示します。

<Sysname> display snmp-agent group

```
Group name:groupv3
Security model:v3 noAuthnoPriv
Readview:ViewDefault
Writeview:<no specified>
Notifyview:<no specified>
Storage-type:nonVolatile
ACL name:testacl
```

表 4-2 コマンド出力

フィールド	説明
Group name	SNMPグループ名
Security model	SNMPグループ構成のセキュリティモード。バージョン情報とセキュリティモードをスペースで区切って指定します。 ● バージョンSNMPv1およびSNMPv2cの場合、認証暗号化レベルはnoAuthNoPrivのみです(認証なし暗号化なし)。 ● バージョンSNMPv3のセキュリティモードは、authPriv (認証と暗号化)、authNoPriv (認証のみ暗号化なし)、noAuthNoPriv (認証なし暗号化なし)の3つです。
Readview	SNMPグループに対応する読み取り専用のMIBビューです。
Writeview	SNMPグループに対応する書き込み可能なMIBビューです。
Notifyview	SNMPグループに対応するTrapおよびInform情報を送信できるMIBビューです。
Storage-type	ストレージの種類は、volatile、nonVolatile、permanent、readOnly、otherです。
ACL	使用されるIPv4 ACLリストの数(このフィールドは、SNMPグループがIPv4 ACL番号にバインドされている場合にのみ表示されます。)
ACL name	使用するACLリスト名(このフィールドは、SNMPグループがACL名にバインドされている場合にのみ表示されます。)
IPV6 ACL	使用されるIPv6 ACLリストの数(このフィールドは、SNMPグループがIPv6 ACLにバインドされている場合にのみ表示されます。)
IPV6 ACL name	使用されているIPv6 ACLリスト名(このフィールドは、SNMPグループがIPv6 ACL名にバインドされている場合にのみ表示されます。)

関連コマンド

- snmp-agent group

4.1.3 display snmp-agent local-engineid

Syntax

display snmp-agent local-engineid

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent local-engineid コマンドは、このデバイスの SNMP エンジン ID を表示します。

例

#このデバイスの SNMP エンジン ID を表示します。

<Sysname> display snmp-agent local-engineid

SNMP local engine ID:800063 A 2800084 E 52 BED 7900000001

関連コマンド

- snmp-agent local-engineid

4.1.4 display snmp-agent mib-view

Syntax

display snmp-agent mib-view [**exclude** |**include** |**viewname** *view-name*]

View

すべての View

デフォルトのユーザロール

network-admin

network-operator

パラメータ

exclude:exclude 属性を持つ MIB ビューの情報を表示します。

include:include 属性を持つ MIB ビューの情報を表示します。

viewname *view-name*:指定した名前の MIB ビューの情報を表示します。*view-name* はビュー名、1~32 文字の文字列で、大文字と小文字が区別されます。

説明

display snmp-agent mib-view コマンドは、MIB ビューの情報を表示します。

パラメータを指定しない場合は、すべての MIB ビューの情報が表示されます。

例

#デバイスのすべての MIB ビューを表示します。

<Sysname> display snmp-agent mib-view

```
View name: ViewDefault
MIB Subtree:iso
Subtree mask:
Storage-type: nonVolatile
View Type: included
View status: active

View name: ViewDefault
MIB Subtree: snmpUsmMIB
Subtree mask:
Storage-type: nonVolatile
View Type: excluded
View status: active

View name: ViewDefault
MIB Subtree: snmpVacmMIB
Subtree mask:
Storage-type: nonVolatile
View Type: excluded
View status: active

View name: ViewDefault
MIB Subtree: snmpModules.18
Subtree mask:
Storage-type: nonVolatile
View Type: excluded
View status: active
```

上記の情報は、デバイスに現在 4 つの MIB ビューがあり、すべて ViewDefault という名前であることを示しています。ViewDefault ビュー名を使用して NMS アクセスを制限する場合、snmpUsmMIB、snmpVacmMIB、および snmpModules.18 サブツリーの下の MIB オブジェクトを除いて、NMS は iso サブツリーの下の他のすべての MIB オブジェクトにアクセスできます。

表 4-3 コマンド出力

フィールド	説明
View name	ビュー名
MIB Subtree	MIBビューに対応するMIBサブツリー
Subtree mask	MIBサブツリーのマスク
Storage-type	ストレージの種類は、volatile、nonVolatile、permanent、readOnly、otherです。
View Type	MIBビューのタイプ(このビューとMIBサブツリーの関係)は、以下の2種類です。 ● includedは、現在のビューにサブツリーのすべてのノードが含まれていることを意味します。つまり、サブツリー内のすべての MIB オブジェクトにアクセスできます。 ● excludedは、現在のビューにサブツリーのノードが含まれていないことを意味します。つまり、サブツリーのすべての MIB オブジェクトにアクセスできません。
View status	MIBビューの状態: ● activeは、MIBビューが使用可能であることを示します。 ● inactiveは、MIBビューが使用できないことを示します。ユーザは、この状態のMIBビュー内のノードに対して読み取り/書き込み操作を実行できませんが、MIB ビューのノードは Trap および Inform メッセージを送信できます。

関連コマンド

- snmp-agent mib-view

4.1.5 display snmp-agent statistics

Syntax

display snmp-agent statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent statistics コマンドは SNMP メッセージの統計情報を表示します。

例

#SNMP メッセージの統計情報を表示します。

<Sysname> display snmp-agent statistics

```
1684 messages delivered to the SNMP entity.
5 messages were for an unsupported version.
0 messages used an unknown SNMP community name.
0 messages represented an illegal operation for the community supplied.
0 ASN.1 or BER errors in the process of decoding.
1679 messages passed from the SNMP entity.
0 SNMP PDUs had badValue error-status.
0 SNMP PDUs had genErr error-status.
0 SNMP PDUs had noSuchName error-status.
0 SNMP PDUs had tooBig error-status (Maximum packet size 1500).
16544 MIB objects retrieved successfully.
2 MIB objects altered successfully.
7 GetRequest-PDU accepted and processed.
7 GetNextRequest-PDU accepted and processed.
1653 GetBulkRequest-PDU accepted and processed.
1669 GetResponse-PDU accepted and processed.
2 SetRequest-PDU accepted and processed.
0 Trap PDUs accepted and processed.
0 alternate Response Class PDUs dropped silently.
0 forwarded Confirmed Class PDUs dropped silently.
```

表 4-4 コマンド出力

フィールド	説明
messages delivered to the SNMP entity	Agent受信したメッセージ数
messages were for an unsupported version	バージョンでサポートされていないメッセージの数
messages used an unknown SNMP community name	不明なSNMPコミュニティ名が使用されたメッセージ数。
messages represented an illegal operation for the community supplied	コミュニティを実行する権限がないオペレーションが運ばれたメッセージ数。
ASN.1 or BER errors in the process of decoding	復号化の間にASN.1あるいはBERエラーがあるメッセージ数。
messages passed from the SNMP entity	SNMPエージェントによって送信されたメッセージ数。
SNMP PDUs had badValue error-status	BadValueエラーのPDU数です。
SNMP PDUs had genErr error-status	genErr誤ったパケット数
SNMP PDUs had noSuchName error-status	NoSuchNameエラーのPDU数です。

フィールド	説明
SNMP PDUs had tooBig error-status	TooBigエラーのPDU数です。（最大パケットサイズが1500バイトです）
MIB objects retrieved successfully	正常に取得されたMIBオブジェクトの数
MIB objects altered successfully	正常に変更されたMIBオブジェクトの数
GetRequest-PDU accepted and processed	受信して処理したGetリクエストの数
GetNextRequest-PDU accepted and processed	受信して処理したGetNextリクエストの数
GetBulkRequest-PDU accepted and processed	受信して処理したGetBulkリクエストの数
GetResponse-PDU accepted and processed	受信して処理したGetレスポンスの数
SetRequest-PDU accepted and processed	受信して処理したSetリクエストの数
Trap PDUs accepted and processed	受信して処理したTrapとInformメッセージの個数
alternate Response Class PDUs dropped silently	破棄された応答パケットの数
forwarded Confirmed Class PDUs dropped silently	ドロップされた転送パケット数

4.1.6 display snmp-agent sys-info

Syntax

display snmp-agent sys-info [**contact** |**location** |**version**]*

View

すべての view

デフォルトのユーザロール

network-admin

network-operator

パラメータ

contact: システム連絡先を表示します。

location: 装置の所在地を表示します。

version: SNMP エージェントのバージョンを表示します。

説明

display snmp-agent sys-info コマンドは SNMP エージェントシステムの情報を表示します。

パラメータを指定しない場合、すべての SNMP エージェントシステムの情報を表示します。

例

#デバイスのシステム情報を表示します。

<Sysname> display snmp-agent sys-info

```
The contact information of the agent:

The location information of the agent:

The SNMP version of the agent:
SNMPv3
```

関連コマンド

- snmp-agent sys-info

4.1.7 display snmp-agent trap queue

Syntax

display snmp-agent trap queue

View

すべての view

デフォルトのユーザロール

network-admin

network-operator

説明

display snmp-agent trap queue コマンドは trap キューの基本情報を表示します。

例

#現在のアラームキューの設定と使用状況を表示します。

<Sysname> display snmp-agent trap queue

```
Queue size:100
Message number:6
```

表 4-5 コマンド出力

フィールド	説明
Queue size	トラップキューの長さ
Message number	トラップメッセージキュー内の現在のトラップメッセージの数

関連コマンド

- snmp-agent trap life
- snmp-agent trap queue-size

4.1.8 display snmp-agent trapbuffer drop

Syntax

display snmp-agent trapbuffer drop

View

すべての view

デフォルトのユーザロール

network-admin

network-operator

説明

display snmp-agent trapbuffer drop コマンドは、SNMP アラーム情報のドロップレコードを表示するために使用されます。

SNMP トラップ情報送信キューが SNMP トラップを破棄すると、トラップの関連情報が SNMP トラップバッファーに記録されるため、ユーザは問題を照会して特定することができます。

例

SNMP トラップの破棄状況を表示します。

<Sysname> display snmp-agent trapbuffer drop

```
Current messages:1
```

（省略）

関連コマンド

- reset snmp-agent trapbuffer

4.1.9 display snmp-agent trapbuffer send

Syntax

display snmp-agent trapbuffer send

View

すべての view

デフォルトのユーザロール

network-admin

network-operator

説明

display snmp-agent trapbuffer send コマンドは、SNMP トラップ情報の送信レコードを表示するために使用されます。

SNMP は、アラートを送信すると、Notification、アラートの送信先 IP、送信結果(成功、失敗)などのアラートの送信情報を SNMP トラップバッファーに記録し、ユーザが質問して問題を特定できるようにします。

例

#SNMP トラップ情報の送信履歴を表示します。

<Sysname> display snmp-agent trapbuffer send

```
Current messages:2
```

（省略）

表示される情報のうち、Current messages は、SNMP Trapbuffer で SNMP トラップ情報を送信したレコードの総数を示します。

関連コマンド

- reset snmp-agent trapbuffer

4.1.10 display snmp-agent trap-list

Syntax

display snmp-agent trap-list

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent trap-list コマンドを使は、SNMP トラップ機能の有効状態を表示します。

モジュールに複数のサブモジュールが含まれる場合、いずれかのサブモジュールのトラップ情報が有効になっている限り、モジュール全体が有効であると表示されます。

snmp-agent trap enable? コマンドを実行することで、サービスモジュールが SNMP トラップ機能をサポートしているかどうか調べることができます。このコマンドによって表示される情報は、**snmp-agent trap enable** コマンドとサービス モジュールの設定に関連しています。

例

SNMP トラップ機能の有効状態を表示します。

<Sysname> display snmp-agent trap-list

```
arp notification is disabled.
```

(省略)

関連コマンド

- snmp-agent trap enable

4.1.11 display snmp-agent usm-user

Syntax

display snmp-agent usm-user [**engineid** *engineid* |**group** *group-name* |**username** *user-name*]*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

engineid *engineid*：指定されたエンジン ID の SNMPv3 ユーザ情報を表示します。*engineid* は SNMP エンジン ID を表し、大文字と小文字は区別されません。SNMPv3 ユーザが作成されると、システムはデバイスの SNMP エンティティエンジン ID を記録します。デバイスのエンジン ID が変更された場合、作成された SNMPv3 ユーザはに無効になります。エンジン ID が復元された後にのみ、有効になります。

group *group-name*：指定した SNMP グループに属する SNMPv3 ユーザに関する情報を表示します。グループ名は大文字と小文字を区別します。

username *user-name*：指定した SNMPv3 ユーザ情報を表示します。ユーザ名は大文字と小文字を区別します。

説明

display snmp-agent usm-user コマンドは、SNMPv3 ユーザ情報を表示します。

snmp-agent usm-user コマンドは SNMPv1/v2c/v3 ユーザを作成することができます。SNMPv1/v2c ユーザが作成されると、システムは同じ名前の新しいコミュニティ名を自動的に追加し、このユーザは SNMPv1/ v2c コミュニティとして処理されます。したがって、display snmp-agent usm-user コマンドを使用して SNMPv1/v2c ユーザ情報を表示することはできません。 SNMPv1/v2c ユーザ情報は display snmp-agent community で表示することができます。

例

#すべての SNMPv3 ユーザの情報を表示します。

<Sysname> display snmp-agent usm-user

```
Username: userv3
Group name: mygroupv3
Engine ID: 800063 A203000FE240A1A6
Storage-type: nonVolatile
UserStatus: active
ACL: 2900

Username: userv3
Group name: mygroupv3
Engine ID: 8000259503000 BB3100A508
Storage-type: nonVolatile
UserStatus: active
ACL name: testacl

Username: userv3code
Role name: groupv3code
network-operator
Engine ID: 800063 A203000FE240A1A6
Storage-type: nonVolatile
UserStatus: active

Username: userv3code
Role name: snmprole
network-operator
Engine ID: 800063 A280000002BB0001
Storage-type: nonVolatile
UserStatus: active
```

表 4-6 コマンド出力

フィールド	説明
Username	SNMPユーザのユーザ名
Group name	SNMPユーザが存在するグループのグループ名
Role name	SNMPユーザの役割名
Engine ID	SNMPユーザ作成時に使用されるSNMPエンティティエンジンID
Storage-type	ストレージの種類は、volatile、nonVolatile、permanent、readOnly、otherです。

フィールド	説明
UserStatus	SNMPユーザのステータスは、次のとおりです。 • active:有効 • notInService:現在使用できません • notReady:設定未完了 • other:その他の状態
ACL	使用されるACLリストの番号(このフィールドは、ユーザがACL番号にバインドされている場合にのみ表示されます。)
ACL name	使用するACLリストの名前(このフィールドは、ユーザがACL名にバインドされている場合にのみ表示されます。)
IPV6 ACL	使用されるIPv6 ACLリストの数(このフィールドは、ユーザがIPv6 ACL番号にバインドされている場合にのみ表示されます。)
IPV6 ACL name	使用されているIPv6 ACLリストの名前(このフィールドは、ユーザがIPv6 ACL名にバインドされている場合にのみ表示されます。)

関連コマンド

- snmp-agent usm-user v3

4.1.12 enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

enable snmp trap updown コマンドは、インターフェースのリンク状態の通知を有効にします。

undo enable snmp trap updown コマンドは、インターフェースのリンク状態の通知を無効にします。

状態が変更したとき、インターフェースで linkUp/linkDown の通知を作成する場合、**snmp-agent trap enable standard** [**linkdown** | **linkup**] *コマンドを使用してグローバルに linkUp/linkDown 通知機能を有効にする必要があります。

例

GigabitEthernet 1/0/1 で linkUp/linkDown の SNMP trap を 10.1.1.1 に送信することを有効にします。コミュニティ名は **public** を使用します。

関連コマンド

- snmp-agent target-host
- snmp-agent trap enable

4.1.13 reset snmp-agent trapbuffer

Syntax

reset snmp-agent trapbuffer

View

User-view

定義済みユーザロール

network-admin

説明

reset snmp-agent trapbuffer コマンドは、SNMP Trapbuffer 内のすべてのレコードを削除します。

例

#SNMP Trapbuffer のすべてのレコードを削除します。

<Sysname> reset snmp-agent trapbuffer

関連コマンド

- display snmp-agent trapbuffer drop
- display snmp-agent trapbuffer send

4.1.14 simulate snmp-trap

🕮 メモ：

simulate snmp-trap コマンドはソフトウェアバージョン 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

simulate snmp-trap all [**ifindex** *ifindex*]

simulate snmp-trap trap-node *name-string* [**context** *context-name*] [**variable-binding** { *variable-binding-name* { **hex** *hex-value* | **null-string** | *variable-binding-value* } } &<1-n>]

View

System view

定義済みユーザロール

network-admin

パラメータ

all：すべての SNMP 通知を指定します。

ifindex *ifindex*: SNMP 通知で送信される ifindex バインド（ノードとも呼ばれます）の値を指定します。値は、装置に存在する任意のインタフェースのインデックスにすることができます。このパラメータを指定しない場合、既存のインタフェースのインデックスを自動的に選択します。

trap-node *name-string*: SNMP 通知ノードを名称もしくは OID で指定します。このパラメータは大文字と小文字を区別しません。1～255 文字で既存のノードを指定してください。

context *context-name*: SNMP コンテキストを指定します。大文字と小文字を区別します。1～32 文字で指定してください。いくつかの通知ノードは異なるシナリオで使用できます。このパラメータは通知が引き起こされる特定のシナリオを示すために使用されます。

variable-binding { *variable-binding-name* { **hex** *hex-value* | **null-string** | *variable-binding-value* } } &<1-n> : SNMP 通知で送信される多様なバインドを指定します。

- *variable-binding-name*: 変数名もしくは OID を指定します。大文字と小文字は区別せず、通知ノードにサポートされる必要があります。
- **hex** *hex-value*: 16 進数形式で指定します。大文字と小文字は区別しません。1～255 の 16 進数で指定します。値は偶数にする必要があります。ベストプラクティスとして、16 進数以外の文字列として変数の値を設定します。ただし、変数値に文字列として直接表現できない特殊文字が含まれている場合は、値を 16 進数形式で設定します。変数バインド値を 16 進数形式で設定する場合は、最初に文字を ASCII コードに変換してから、ASCII コードを 16 進値に変換してください。
- **null-string**: 変数のバインドがヌル文字列であることを示します。

- *variable-binding-value*: 変数を 16 進数ではない形式で指定します。大文字と小文字を区別しません。1 から 255 の 16 進数文字ではない文字列です。
- &<1-n>: 最大 n 個の変数バインドを指定できることを示します。n の値は、通知ノードによって異なります。

説明

simulate snmp-trap コマンドは SNMP 通知送信をシミュレートします。

1) アプリケーションシナリオ
この機能は SNMP 通知機能が正常かどうか、通知設定が正しいか、NMS が通知を受信し正常に解析できるかどうかをテストできます。NMS が SNMP 通知を受信できない場合、問題を特定し、解決するためのトラブルシューティングを実施します。
2) 動作メカニズム
この機能を設定すると、装置は各ノードのメッセージを含む SNMP 通知を生成し、生成した通知を SNMP モジュールから送信します。
生成された SNMP 通知で送信されるノードは、以下のような値が割り当てられます。

- **数字タイプノード**—ノードの範囲の最小値を指定します。値の範囲がないノードには、0 が割り当てられます。
- **文字タイプノード**—値は Test です。文字数の指定要件がある場合、要件を満たすまで“Test”を切り捨てるか、繰り返します。
- **タイムスタンプタイプノード**—現在のシステム時刻を指定します。
- **IPv4 アドレスタイプノード**—“127.0.0.1”を指定します。
- **ビットタイプノード**—ノードのデフォルト値を使用します。デフォルト値がないノードの場合、ノードの設定範囲の最小値を使用します。
- **パスワードタイプノード**—値は“******”です。
- **オブジェクト識別子ノード**—値は通知の OID です。

同じイベントの通知とリカバリ通知は順番に送信されます。
通知ノードに同じ名前の変数が複数含まれている場合、同一の変数と値を順番に指定してください。変数に値を指定しない場合、上記の規則に基づいて値が割り当てられます。

この機能を有効にする前に、SNMP を有効にする必要があります。また、通知が送信されるようにするために、**snmp-agent target-host** コマンドを実行し、SNMP 通知のターゲットホストを指定してください。必要に応じて別の SNMP パラメータを設定してください。

このコマンドを設定するためのヘルプ情報を取得するには、コマンドの特定のパラメーター位置に「?」を入力します。たとえば、デバイスでサポートされているトラップ通知を取得するには、simulate snmp-trap trap-node ? のようにコマンドに「?」と入力します。

例

サポートされているすべての SNMP 通知の送信をシミュレートします。

<AC> system-view

[AC] simulate snmp-trap all

```
This operation will take long time and is resources-intensive. Continue?[Y/N]:y
```

linkUP SNMP 通知の送信をシミュレートします。

<AC> system-view

[AC] simulate snmp-trap trap-node linkUP

OID 1.3.6.1.6.3.1.1.5.4 (linkUp) を使用した SNMP 通知の送信をシミュレートします。OID 1.3.6.1.2.1.2.2.1.1 (ifIndex) の変数と OID 1.3.6.1.2.1.2.2.1.7 の変数 (ifAdminStatus) を送信するように通知を設定し、両方の変数の値を 1 に設定します。

<AC> system-view

[AC] simulate snmp-trap trap-node 1.3.6.1.6.3.1.1.5.4 variable-binding 1.3.6.1.2.1.2.2.1.1 1 1.3.6.1.2.1.2.2.1.7 1

関連コマンド

- **snmp-agent**
- **snmp-agent target-host**

4.1.15 snmp-agent

Syntax

snmp-agent

undo snmp-agent

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

snmp-agent コマンドは SNMP エージェントを有効にします。

undo snmp-agent コマンドは SNMP エージェントを無効にします。

snmp-agent calculate-password を除く **snmp-agent** で始まるコマンドを実行するとき、SNMP エージェントは自動で有効になります。

SNMP リスニング ポートがデバイス上の他のサービスによって使用されている場合、SNMP 機能は開始に失敗します。SNMP リスニング ポートは、snmp-agent port コマンドで設定できます.ユーザは、display udp verbose コマンドを使用して、デバイスの UDP ポートの使用状況を確認できます.

ユーザが SNMP モジュールの関連する構成を変更した後、SNMP エージェント機能が無効になっていると、構成は一時的に有効になりません。display current-configuration コマンドを実行しても、これらのコマンドは表示されず、save コマンドを実行しても、これらの設定は設定ファイルに保存されません。SNMP エージェント機能を有効にすると、これらの設定はすぐに有効になり、繰り返し設定する必要はありません。

例

#デバイスの SNMP Agent 機能を有効にします。

<Sysname> system-view

[Sysname] snmp-agent

関連コマンド

- display udp verbose
- snmp-agent port

4.1.16 snmp-agent { inform | trap } source

Syntax

snmp-agent { **inform** | **trap** } **source** *interface-type* {*interface-number* |*interface-number.subnumber* }

undo snmp-agent { **inform | trap** } **source**

デフォルト

送信元インターフェース IP アドレス

View

System-view

定義済みユーザロール

network-admin

パラメータ

inform:Inform パケットの送信元 IP アドレスを指定します。

trap:Trap パケットの送信元 IP アドレスを指定します。

interface-type {*interface-number* |*interface-number.subnumber* }:レイヤ 3 インターフェース番号とインターフェースタイプを指定します。ここで、interface-number はプライマリインターフェイス番号です。subnumber はサブインターフェース番号で、値の範囲は 1~4094 です。

説明

snmp-agent {**inform** |**trap** } **source** コマンドを使用は、送信されるトラップ情報の送信元 IP アドレスを設定します。

undo snmp-agent {**inform** |**trap** } **source** コマンドを使用は、デフォルトに戻します。

このコマンドを実行すると、指定したインターフェースのプライマリ IP アドレスが、送信されるトラップ情報の送信元 IP アドレスとして使用されます。このように、IP アドレスを使用して、NMS 上のエージェントを一意に識別できます。エージェントが異なるアウトバウンド インターフェースを使用してトラップ情報を送信する場合でも、NMS はこの IP アドレスを使用して、エージェントが送信するすべてのトラップ情報をフィルタリングできます

トラップ情報を取得するための送信元アドレスインターフェースとしてインターフェースを設定する前に、次の点に注意してください。

- 構成されたインターフェースがすでに存在し、正当な IP アドレスが構成されている場合、その IP アドレスがトラップ情報の送信元アドレスとして使用されます。
- 設定されたインターフェースが存在しない場合、このコマンドは設定に失敗します。
- 設定されたインターフェースがすでに存在し、有効な IP アドレスが設定されていない場合、このコマンドは有効ではなく、インターフェースに有効な IP アドレスが設定されると自動的に有効になります。

例

#Trap パケットの送信元アドレスを VLAN インターフェース 1 のプライマリ IP アドレスに設定します。

<Sysname> system-view

[Sysname] snmp-agent trap source vlan-interface 1

＃Inform パケットの送信元アドレスを、VLAN インターフェース 2 のプライマリ IP アドレスとして設定します。

<Sysname> system-view

[Sysname] snmp-agent inform source vlan-interface 2

関連コマンド

- snmp-agent trap enable
- snmp-agent target-host

4.1.17 snmp-agent calculate-password

Syntax

snmp-agent calculate-password plain-password *mode* {**3 desmd5** |**3 dessha** |**aes192md5** |**aes192sha** |**aes256md5** |**aes256sha** |**md 5**|**sha**} {**local-engineid** |**specified-engineid** *engineid* }

View

System-view

定義済みユーザロール

network-admin

パラメータ

plain-password: プレーンテキスト形式のキーを指定します。大文字と小文字を区別する 1～64 文字の文字列です。

mode:認証アルゴリズムと暗号化アルゴリズムを指定します。デバイスでサポートされている認証アルゴリズムは HMAC-MD5 と HMAC-SHA1 で、HMAC-MD5 は HMAC-SHA1 より計算が速く、HMAC-SHA1 は HMAC-MD5 よりセキュリティが高いです。サポートする暗号アルゴリズムの安全性は高い順に AES256、AES192、AES、3 DES、DES です。セキュリティの高いアルゴリズムは計算が遅くなります。DES アルゴリズムは、一般的なセキュリティ要件を満たすことができます。

- 3 desmd5:暗号文の暗号文の計算に使用されます。対応する認証アルゴリズムは HMAC-MD5、暗号化アルゴリズムは 3 DES である必要があります。
- 3 dessha:暗号文暗号文の計算に使用されます。対応する認証アルゴリズムは HMAC-SHA1、暗号化アルゴリズムは 3 DES である必要があります。
- aes192md5:暗号文の暗号化パスワードの計算に使用されます。対応する認証アルゴリズムは HMAC-MD5、暗号化アルゴリズムは AES192 である必要があります。
- aes192sha:暗号文の暗号化パスワードの計算に使用されます。対応する認証アルゴリズムは HMAC-SHA1、暗号化アルゴリズムは AES192 である必要があります。
- aes256md5:暗号文の暗号化パスワードの計算に使用されます。対応する認証アルゴリズムは HMAC-MD5、暗号化アルゴリズムは AES256 である必要があります。
- aes256sha:暗号文の暗号化パスワードの計算に使用されます。対応する認証アルゴリズムは HMAC-SHA1、暗号化アルゴリズムは AES256 である必要があります。
- md 5:暗号文認証パスワードと暗号文の暗号化パスワードの計算に使用します。暗号文認証パスワードの計算に使用する認証アルゴリズムは HMAC-MD5 である必要があります。暗号文の暗号化に使用する暗号文は、認証アルゴリズムが HMAC-MD5、暗号化アルゴリズムが AES または DES である必要があります。認証アルゴリズムが HMAC-MD5 の場合、同じ平文暗号でも、それぞれ計算される暗号文認証暗号と暗号文暗号は同じであるからである。
- sha:暗号文認証パスワードと暗号文の暗号化パスワードの計算に使用します。暗号文認証パスワードの計算に使用する認証アルゴリズムは HMAC-SHA1 である必要があります。暗号文の暗号化に使用する暗号文は、認証アルゴリズムが HMAC-SHA1、暗号化アルゴリズムが AES または DES である必要があります。認証アルゴリズムが HMAC-SHA1 の場合、同じ平文暗号でも、それぞれ計算される暗号文認証暗号と暗号文暗号は同じであるからである。

local-engineid: キーの暗号化された形式を計算するためローカルエンジン ID を使用します。snmp-agent local-engineid コマンドでローカルエンジン ID を設定することができます。

specified-engineid *engineid*: キーの暗号化された形式を計算するためユーザ定義のエンジン ID を使用します。engineid は 16 進数の文字列で SNMP エンジン ID を指定しま

す。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。

説明

snmp-agent calculate-password コマンドは、平文パスワードに対応する暗号文パスワードを計算するために使用します。

このコマンドを実行する前に、デバイスの SNMP Agent 機能を有効にする必要があります。

SNMPv3 ユーザの作成時に、認証または暗号化されたパスワードを暗号文に指定すると、平文のパスワードの代わりにこのコマンドによって生成された暗号文パスワードを入力することができます。これにより、セキュリティ保護されていない環境で平文のパスワードを直接入力することによるセキュリティ上の問題を回避できます。

生成されたパスワードはエンジン ID に関連付けられており、エンジン ID で生成されたパスワードは、このエンジン ID でのみ有効になります。

例

#ローカルエンジン ID と HMAC-SHA1 アルゴリズムを使用して、平文の認証パスワード authkey の暗号化テキストパスワードを計算します。

<Sysname> system-view

[Sysname] snmp-agent calculate-password authkey mode sha local-engineid

```
The encrypted key is:09659 EC5A9AE91BA189E5845E1DDE0CC
```

関連コマンド

- snmp-agent local-engineid
- snmp-agent usm-user v3

4.1.18 snmp-agent community

Syntax

VACM 方式:

snmp-agent community {**read** |**write** } [**simple** |**cipher**] *community-name* [**mib-view** *view-name*] [**acl** {*ipv4-acl-number* |**name** *ipv4-acl-name* }]*

undo snmp-agent community [**cipher**] *community-name*

RBAC 方式:

snmp-agent community [**simple** |**cipher**] *community-name* **user-role** *role-name* [**acl** {*ipv4-acl-number* |**name** *ipv4-acl-name* }]*

undo snmp-agent community [**cipher**] *community-name*

デフォルト

設定なし

定義済みユーザロール

System-view

パラメータ

read: 指定されたコミュニティを MIB オブジェクトへの読み出し専用のアクセス権限に割り当てます。読み出し専用コミュニティは MIB 情報を問い合わせることのみ可能です。

write: 指定されたコミュニティを MIB オブジェクトへの読み出し、書き込みのアクセス権限に割り当てます。読み出し専用コミュニティは MIB 情報を設定することができます。

simple: プレーンテキストのコミュニティを設定します。セキュリティのため、コミュニティは暗号テキストで保存されます。

cipher: 暗号テキストのコミュニティを設定し、暗号テキストで保存します。

community-name: コミュニティを設定します。大文字、小文字を区別します。プレーンテキストの設定範囲は 1～32 文字です。暗号テキストの設定範囲は 33～73 文字です。バックスラッシュの後にエスケープ文字として文字列を入力します。

mib-view *view-name*: コミュニティで有効な MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。MIB view はアクセス可能な MIB オブジェクトの一式を示します。MIB view を指定しない場合、コミュニティはデフォルト MIB view の ViewDefault の MIB オブジェクトにアクセスできます。

user-role *role-name*:コミュニティのロール名。*role-name* は 1~63 文字の文字列で、大文字と小文字が区別されます。

acl:グループ名を Basic/Advanced IPv4 ACL に指定します。

ipv4-acl-number:基本または拡張 IPv4 ACL を表す番号。ここで、基本 IPv4 ACL は 2000~2999 の値を取り、拡張 IPv4 ACL は 3000~3999 の値を取ります。

name *ipv4-acl-name*:Basic または Advanced IPv4 ACL 名。1~63 文字の文字列で、大文字と小文字は区別されません。

説明

snmp-agent community コマンドは SNMP コミュニティを作成します。

undo snmp-agent community コマンドは SNMP コミュニティを削除します。

このコマンドを実行できるのは、network-admin または level-15 ユーザのみです。

このコマンドは、SNMPv1 および SNMPv2c ネットワーク環境で使用されます。

コミュニティは、コミュニティ名でマークされた NMS とエージェントの集まりです。コミュニティ名はパスワードに相当し、コミュニティ内のデバイス通信はコミュニティ名を認証に使用します。NMS と Agent で設定されたコミュニティ名が同じ場合にのみ、相互にアクセスできます。通常、読み取り権限のコミュニティ名は「public」、書き込み権限のコミュニティ名は「private」を使用します。セキュリティを強化するために、network-admin は他のコミュニティ名も設定できます。

ユーザは次の 2 つの方法でグループを作成できます。

- snmp-agent community コマンドを使用してコミュニティを作成します。
- snmp-agent usm-user { v1 | v2c }および snmp-agent group { v1 | v2c }コマンドを設定して、SNMPv1 または SNMPv2c ユーザと対応するグループ作成後、システムは自動的にユーザ名とコミュニティを作成します。

display snmp-agent community では、これら 2 つの方法で作成され、構成ファイルにクリアテキストで保存されたコミュニティの情報が表示されます。

snmp-agent community コマンドを使用してコミュニティを作成する場合、コミュニティへのアクセスを制御するには 2 つの構成方法があります

- VACM (View-based Access Control Model、ビューベースのアクセス制御モデル)は、MIB ビューを指定することで、NMS がアクセスできる MIB ノードを制限し、読み取り専用/書き込みの両方のアクションを使用して構成されます。
- RBAC (Role Based Access Control、ロールベースアクセスコントロール)は、ユーザロールを使用して NMS へのアクセスを制限するように構成されています。デフォルトでは、ユーザロール network-admin と level-15 はすべての MIB ノードを読み取り/書き込みでき、network-operator はすべての MIB ノードの読み取りを行うことができます。ユーザロールの詳細については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*2 基本機能*”の”*2 章 RBAC*”を参照してください。

このコマンドにより最大 10 個のコミュニティを作成することができます。

コミュニティ名が同じでパラメータが異なる場合新しい設定が有効になります。

simple パラメータと cipher パラメータを指定しない場合は、コミュニティ名がクリアテキストで設定され、設定ファイルにクリアテキストで保存されます。

acl パラメータを使用することで、不正な NMS アクセスデバイスを制限できます。

- ACL が参照されていない場合、参照した ACL が存在しない場合、または参照した ACL にルールが設定されていない場合、すべての NMS がデバイスにアクセスできます。
- 参照された ACL でルールが設定されている場合、ルールで許可されている NMS のみがデバイスにアクセスでき、他の NMS はデバイスにアクセスできません。

ACL の詳細な説明と説明については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。

例

SNMP コミュニティ readaccess をクリアテキストで作成し、NMS がデバイスのデフォルト ビューで MIB オブジェクトへの読み取り専用アクセスにコミュニティ名を使用できるようにします。

<Sysname> system-view

[Sysname] snmp-agent sys-info version v1 v2c

[Sysname] snmp-agent community read simple readaccess

#コミュニティ名 writeaccess をクリアテキストで構成し、IP アドレス 1.1.1.1 を持つ NMS のみがそのコミュニティ名を使用してデバイスのデフォルトビュー内の MIB オブ

ジェクトに対する読み取り/書き込みを許可し、他の NMS はそのコミュニティ名を使用した書き込みを禁止します。

<Sysname> system-view

[Sysname] acl basic 2900

[Sysname-acl-ipv4-basic-2900] rule permit source 1.1.1.1 0.0.0.0

[Sysname-acl-ipv4-basic-2900] rule deny source any

[Sysname-acl-ipv4-basic-2900] quit

[Sysname] snmp-agent sys-info version v2c

[Sysname] snmp-agent community write simple writeaccess acl 2900

#コミュニティ名 writeaccess をクリアテキストで構成し、IP アドレス 1.1.1.2 を持つ NMS のみがそのコミュニティ名を使用してデバイスのデフォルトビュー内の MIB オブジェクトに対する読み取り/書き込みを許可し、他の NMS はそのコミュニティ名を使用した書き込みを禁止します。

<Sysname> system-view

[Sysname] acl basic name testacl

[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0

[Sysname-acl-ipv4-basic-testacl] rule deny source any

[Sysname-acl-ipv4-basic-testacl] quit

[Sysname] snmp-agent sys-info version v2c

[Sysname] snmp-agent community write simple writeaccess acl name testacl

#グループ名 wr-sys-acc をクリアテキストで作成します。このグループ名を使用してデバイスにアクセスすると、system (OID は 1.3.6.1.2.1.1 です。)サブツリーの下にある MIB オブジェクトに対してのみ書き込み操作を実行できます。

<Sysname> system-view

[Sysname] snmp-agent sys-info version v1 v2c

[Sysname] undo snmp-agent mib-view ViewDefault

[Sysname] snmp-agent mib-view included test system

[Sysname] snmp-agent community write simple wr-sys-acc mib-view test

関連コマンド

- display snmp-agent community
- snmp-agent mib-view

4.1.19 snmp-agent group

Syntax

SNMPv1、SNMPv2c：

snmp-agent group {**v 1**|**v 2 c**} *group-name* **[notify-view** *view-name* |**read-view** *view-name* |**write-view** *view-name*]*[**acl** {*ipv4-acl-number* |**name** *ipv4-acl-name* }]*

undo snmp-agent group {**v 1**|**v 2 c**} *group-name*

SNMPv3：

snmp-agent group v3 *group-name* [**authentication** |**privacy**] [**notify-view** *view-name* |**read-view** *view-name* |**write-view** *view-name*]*[**acl** {*ipv4-acl-number* |**name** *ipv4-acl-name* }]*

undo snmp-agent group v3 *group-name* [**authentication** |**privacy**]

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

group-name: SNMP グループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

authentication:プライバシーなしのモデルを指定します。

privacy:プライバシーセキュリティモデルを指定します。

notify-view view-name: notify の MIB view **を指定します。**view-name **は** MIB view **の名**前を示します。設定範囲は 1～32 文字で、大文字と小文字が区別されます。SNMP エージェントは notify view に含まれる MIB オブジェクトのため、指定されたグループのみのユーザに通知を送信します。

read-view *view-name*:1~32 文字の文字列で、大文字と小文字が区別されます。デフォルト値は ViewDefault です。

write-view *view-name*: 読み込み、書き込みの MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。読み込み、書き込みの MIB view を

指定しない場合、SNMP グループは SNMP エージェントの MIB オブジェクトを設定することができません。

acl:グループを標準または拡張 IPv4 ACL にバインドします。

ipv4-acl-number:標準または拡張 IPv4 ACL 番号。ここで、標準 IPv4 ACL 番号は 2000 から 2999 までの値を取り、拡張 IPv4 ACL 番号は 3000~3999 までの値を取ります。

name *ipv4-acl-name*:標準または拡張 IPv4 ACL 名。1~63 文字の文字列で、大文字と小文字は区別されません。

説明

snmp-agent group コマンドは SNMP グループを作成します。

undo snmp-agent group コマンドは SNMP グループを削除します。

このコマンドを実行できるのは、network-admin または level-15 のユーザロールを持つユーザのみです。

SNMP グループは、セキュリティモード、ビュー権限などの情報を定義し、グループ内に構成されたすべてのユーザがこれらの共通属性を持ちます。

システムで構成できる SNMP グループの最大数は 20 です。

authentication および privacy パラメータを指定するかどうかは、次のとおりです。

- authentication と privacy を指定しない場合は、認証なしおよび暗号化されていないことを示します。SNMP 接続する場合、認証および暗号化は行われず、ユーザが認証パスワード/暗号化パスワードを設定していても、認証パスワード/暗号化パスワードは有効になりません。
- authentication を指定した場合、認証は暗号化されません。SNMP 接続する場合、認証は暗号化されず、ユーザが暗号化パスワードを設定しても、暗号化パスワードは有効になりません。
- privacy を指定すると、認証は暗号化されます。SNMP 接続すると、暗号化が認証されます。グループ内のユーザは、認証パスワードと暗号化パスワードを設定する必要があります。設定していない場合、SNMP 接続できません。

acl パラメータを使用して、不正な NMS アクセスを制限できます。グループまたはユーザを作成する場合、ACL は次のルールに従います。

- 参照されていない ACL、参照されている ACL が存在しない場合、または参照されている ACL にルールが設定されていない場合は、すべての NMS がデバイスにアクセスできるようにします。
- 参照 ACL でルールが設定されている場合、ルール内の permit の NMS のみがデバイスにアクセスでき、他の NMS はデバイスにアクセスできません。

ACL の詳細な説明と説明については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。

例

#SNMPv3 を実行しているデバイス上に SNMP グループ group1 を作成します。

<Sysname> system-view

[Sysname] snmp-agent group v3 group1

関連コマンド

- display snmp-agent group
- snmp-agent mib-view
- snmp-agent usm-user

4.1.20 snmp-agent local-engineid

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

デフォルト

ローカルエンジン ID は company ID と device ID の組み合わせです。

View

System-view

定義済みユーザロール

network-admin

パラメータ

engineid:SNMP エンジン ID は 16 進数で指定する必要があり、10~64 の範囲で指定できます。大文字と小文字は区別されず、0 と F は使用できません。

説明

snmp-agent local-engineid コマンドはローカル SNMP エージェントの SNMP エンジン ID を変更します。

undo snmp-agent local-engineid コマンドはデフォルトに戻します。

SNMP エンジン ID には、次の 2 つの機能があります。

- NMS で管理されているすべてのデバイスでは、各デバイスは一意のエンジン ID で Agent を識別します。ネットワーク管理者は、管理ドメイン内で重複するエンジン ID がないことを確認する必要があります。
- SNMPv3 のユーザ名、暗号文パスワードはエンジン ID に関連付けられており、エンジン ID を変更すると、元のエンジン ID で設定されたユーザ名、パスワードが無効になります。

ユーザは、ネットワーク全体の構成に従って、覚えやすいエンジン ID をデバイスに設定することができます。

例

#このデバイスの SNMP エンジン ID を 123456789 A に設定します。

<Sysname> system-view

[Sysname] snmp-agent local-engineid 123456789A

関連コマンド

- display snmp-agent local-engineid
- snmp-agent usm-user

4.1.21 snmp-agent log

Syntax

snmp-agent log {**all**|**authfail** |**get-operation** |**set-operation** }

undo snmp-agent log {**all**|**authfail** |**get-operation** |**set-operation** }

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

パラメータ

all: SNMP 認証失敗、Get オペレーション、Set オペレーションのロギングを有効にします。

authfail: SNMP 認証の失敗のロギングを有効にします。

get-operation: SNMP Get オペレーションのロギングを有効にします。

set-operation: SNMP Set オペレーションのロギングを有効にします。

説明

snmp-agent log コマンドは SNMP オペレーションのロギングを有効にします。

undo snmp-agent log コマンドは SNMP オペレーションのロギングを無効にします。

NMS のふるまいを検査するため、SNMP エージェントで実行された SNMP オペレーションを記録することができます。SNMP エージェントはログデータを information center に送信します。必要に応じて宛先にデータを出力するように Information Center を設定することができます。

例

#SNMP Get オペレーションのロギングを有効にします。

<Sysname> system-view

[Sysname] snmp-agent log get-operation

#SNMP Set オペレーションのロギングを有効にします。

<Sysname> system-view

[Sysname] snmp-agent log set-operation

#SNMP 認証失敗のロギングを有効にします。

<Sysname> system-view

[Sysname] snmp-agent log authfail

4.1.22 snmp-agent mib-view

Syntax

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

デフォルト

SNMP エージェントが有効なとき、システムは ViewDefault view を作成します。デフォルト MIB view では iso サブツリーのすべての MIB オブジェクトは snmpUsmMIB、snmpVacmMIB、snmpModules.18 サブツリーを除いてアクセス可能です。

View

System-view

定義済みユーザロール

network-admin

パラメータ

excluded: 指定した MIB サブツリーのすべてのノードへのアクセスを拒否します。

included: 指定した MIB サブツリーのすべてのノードへのアクセスを許可します。

view-name: view 名を指定します。設定範囲は 1～32 文字です。

oid-tree: ルートノードの OID（たとえば、1.3.6.1.2.1.1）あるいはオブジェクト名（たとえば、system）によって MIB サブツリーを指定します。oid-tree 引数は、1～255 文字の文字列です。OID は MIB ツリーのオブジェクトを固有に識別するドットで区切られた 10 進数の数字です。

mask *mask-value*: MIB サブツリーのマスクを指定します。16 進数です。マスク長は 1～32 の偶数にする必要があります。

説明

snmp-agent mib-view コマンドは MIB view を作成あるいはアップデートします。

undo snmp-agent mib-view コマンドは MIB view を削除します。

MIB view は、アクセス制限のある MIB オブジェクトの集合（あるいは MIB オブジェクト階層）を示し、view 名によって識別されます。MIB view に含まれる MIB オブジェクトはアクセス可能ですが、MIB view から除外されている MIB オブジェクトはアクセスできません。

各 *view-name oid-tree* は view のレコードを示します。異なる MIB サブツリーのマスクで複数回、同一のレコードを指定する場合、最後に行った設定が適用されます。

システムは、最大 20 個の MIB view のレコードを格納できます。4 つのデフォルト MIB view レコードに加えて、最大 16 個の MIB view レコードを作成できます。**undo snmp-agent mib-view** コマンドを使用してデフォルトビューを削除すると、最大 20 個の MIB view レコードを作成できます。

デフォルト MIB view を削除する場合には注意してください。デフォルト view を使用する NMS から装置の MIB オブジェクトにアクセスできなくなります。

例

mibtest view に mib-2（OID 1.3.6.1.2.1）サブツリーを含め、この view から system サブツリーを除外します。

<Sysname> system-view

[Sysname] snmp-agent sys-info version v1

[Sysname] snmp-agent mib-view included mibtest 1.3.6.1.2.1

[Sysname] snmp-agent mib-view excluded mibtest system

[Sysname] snmp-agent community read public mib-view mibtest

コミュニティ public の SNMPv1 の NMS は mib-2 サブツリーのオブジェクトに問い合わせすることができますが、system サブツリーの他のオブジェクト（たとえば、sysDescr あるいは sysObjectID ノード）は問い合わせすることができません。

関連コマンド

- display snmp-agent mib-view
- snmp-agent group

4.1.23 snmp-agent packet max-size

Syntax

snmp-agent packet max-size byte-count

undo snmp-agent packet max-size

デフォルト

1500 バイト

View

System-view

定義済みユーザロール

network-admin

パラメータ

byte-count: SNMP エージェントが送受信できる SNMP パケットの最大サイズを指定します。設定範囲は 484～17940 バイトです。

説明

snmp-agent packet max-size コマンドは SNMP エージェントが送受信できる SNMP パケットの最大サイズを設定します。

undo snmp-agent packet max-size コマンドはデフォルトに戻します。

NMS へのパス上の装置がパケットのフラグメンテーションをサポートしていない場合、大きいサイズのパケットが廃棄されないようにするため、SNMP パケットサイズを制限します。通常のネットワークではデフォルトの設定で十分です。

例

SNMP パケットの最大サイズを 1024 バイトに設定します。

<AC> system-view

[AC] snmp-agent packet max-size 1024

4.1.24 snmp-agent packet response dscp

Syntax

snmp-agent packet response dscp *dscp-value*

undo snmp-agent packet response dscp

デフォルト

0

View

System-view

定義済みユーザロール

network-admin

パラメータ

dscp-value : SNMP 応答パケットの DSCP 優先度を 0 ～ 63 の範囲で示します。値が大きいほど優先度が高くなります。

説明

snmp-agent packet response dscp コマンドは、SNMP 応答パケットの DSCP 優先度を設定します。

undo snmp-agent packet response dscp コマンドはデフォルトに戻します。

DSCP 優先度は、IP パケットの ToS フィールドにカプセル化され、パケット自体の優先度を示すために使用されます。デバイスは優先度に従ってパケット送信の優先度を決定します。

例

＃SNMP 応答パケットの DSCP 優先度を 40 に設定します。

<Sysname> system-view

[Sysname] snmp-agent packet response dscp 40

4.1.25 snmp-agent sys-info contact

Syntax

snmp-agent sys-info contact *sys-contact*

undo snmp-agent sys-info contact

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

sys-contact: システム連絡先を指定します。設定範囲は 1～255 文字です。

説明

snmp-agent sys-info contact コマンドはシステム連絡先を設定します。

undo snmp-agent sys-info contact コマンドはデフォルトに戻します。

システム管理の連絡先と管理者を設定します

例

システム連絡先を Dial System Operator # 27345 に指定します。

<AC> system-view

[AC] snmp-agent sys-info contact Dial System Operator # 27345

関連コマンド

- display snmp-agent sys-info

4.1.26 snmp-agent sys-info location

Syntax

snmp-agent sys-info location *sys-location*

undo snmp-agent sys-info location

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

sys-location: システム所在地を指定します。設定範囲は 1～255 文字です。

説明

snmp-agent sys-info location コマンドはシステム所在地を設定します。

undo snmp-agent sys-info location コマンドはデフォルトに戻します。

システム管理の装置と管理者の所在地を設定します。

例

システム所在地を Room524-row1-3 に設定します。

<AC> system-view

[AC] snmp-agent sys-info location Room524-row1-3

関連コマンド

- display snmp-agent sys-info

4.1.27 snmp-agent sys-info version

Syntax

snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

undo snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

デフォルト

SNMPv3

View

System view

定義済みユーザロール

network-admin

パラメータ

all: SNMPv1、SNMPv2c、SNMPv3 を指定します。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

説明

snmp-agent sys-info version コマンドは SNMP のバージョンを有効にします。

undo snmp-agent sys-info version コマンドは SNMP のバージョンを無効にします。

NMS が SNMP エージェントと正常に通信するため、SNMP エージェントは NMS と同じ SNMP のバージョンを設定します。

IPv 6 環境で SNMP トラップ機能を使用する場合は、SNMP バージョン番号を v 2 c または v 3 に設定します。

例

SNMPv3 を有効にします。

<AC> system-view

[AC] snmp-agent sys-info version v3

関連コマンド

- display snmp-agent sys-info

4.1.28 snmp-agent target-host

Syntax

snmp-agent target-host inform address udp-domain {*ipv4-target-host* } [**udp-port** *port-number*] **params securityname security-string** {**v 2 c**|**v 3** [**authentication** |**privacy**]}

snmp-agent target-host trap address udp-domain {*ipv4-target-host* } [**udp-port** *port-number*] [**dscp** *dscp-value*] **params securityname** *security-string* [**v 1**|**v 2 c**|**v 3** [**authentication** |**privacy**]]

undo snmp-agent target-host {**trap** |**inform** } **address udp-domain** {*ipv4-target-host* } **params securityname** *security-string*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

inform: inform として通知を送信します。

trap: trap として通知を送信します。

address: SNMP 通知の宛先アドレスを指定します。

udp-domain: トランスポートプロトコルとして UDP を指定します。

ipv4-target-host:トラップ情報を受信する宛先ホストの IPv4 アドレスまたはホスト名。ホスト名は 1~253 文字の文字列で、大文字と小文字は区別されません。文字列には、英字、数字、「-」、「_」、または「.」のみを使用できます。ホスト名を用いて構成すると、送信時にホスト名に対応する IPv 4 アドレスを取得し、対応するホストにトラップパケットを送信する。

udp-port *port-number*: SNMP 通知の UDP ポートを指定します。指定しない場合、UDP ポート 162 が使用されます。

dscp *dscp-value*:宛先ホストに送信される Trap パケットの DSCP 優先度を 0~63 の範囲で設定します。デフォルトは 0 です。値が大きいほど優先度が高くなります。DSCP 優先度は、IP メッセージ内の ToS フィールドにカプセル化され、パケット自体の優先度を示すために使用され、デバイスは優先度に従ってパケット送信の優先度を決定できます。

params securityname security-string: 認証パラメータを指定します。security-string は SNMPv1 コミュニティ、SNMPv2c コミュニティ、あるいは SNMPv3 ユーザ名を指定します。設定範囲は 1〜32 文字です。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

authentication: プライバシーセキュリティなしで認証するようにセキュリティモデルを指定します。SNMPv3 ユーザを作成したとき認証キーを指定する必要があります。

privacy: プライバシーセキュリティありで認証するようにセキュリティモデルを指定します。SNMPv3 ユーザを作成したとき認証キーと暗号化キーを指定する必要があります。

説明

snmp-agent target-host コマンドは SNMP 通知（inform あるいは trap）をホストに送信するため、SNMP エージェントを設定します。

undo snmp-agent target-host コマンドは SNMP 通知のターゲットホストを削除します。

複数の SNMP 通知のターゲットホストを指定することができます。

SNMP エージェントは SNMP 通知のため、ターゲットホストの UDP ポートと同一のポートを使用する必要があります。通常、MIB ブラウザのような NMS は SNMP 通知のために、SNMP プロトコルで定義された UDP ポート 162 を使用します。

v1、v2c、v3 を指定しない場合、SNMPv1 が使用されます。ホストが通知を受信できるように、SNMP エージェントは、ターゲットホストの SNMP のバージョンと同一のバージョンを使用することを確認してください。

authentication あるいは **privacy** の両方を指定しない場合、セキュリティモデルはプライバシーセキュリティなし、認証なしです。

例

ユーザ public の 10.1.1.1 に SNMPv3 の trap を送信するため、SNMP エージェントを設定します。

<AC> system-view

[AC] snmp-agent trap enable standard

[AC] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public v3

関連コマンド

- snmp-agent {inform |trap } source
- snmp-agent trap enable
- snmp-agent trap life

4.1.29 snmp-agent trap enable

Syntax

snmp-agent trap enable [**configuration** |*protocol* |**standard** [**authentication** |**coldstart** |**linkdown** |**linkup** |**warmstart**]*|**system**]

undo snmp-agent trap enable [**configuration** |*protocol* |**standard** [**authentication** |**coldstart** |**linkdown** |**linkup** |**warmstart**]*|**system**]

デフォルト

SNMP configuration 通知、standard 通知、system 通知は有効です。他の SNMP 通知はモジュールによって変わります。

View

System view

定義済みユーザロール

network-admin

パラメータ

configuration: configuration 通知を指定します。configuration 通知が有効である場合、システムはカレントコンフィグレーションとスタートアップコンフィグレーションを 10 分毎に変更点を確認し、最新の変更の通知を作成します。

protocol: SNMP 通知が有効なモジュールを指定します。このパラメータの詳細は各機能のコマンドマニュアルを参照してください。

standard: standard 通知を指定します。

authentication: NMS が SNMP エージェントへの認証に失敗したとき、認証失敗通知を送信します。

coldstart: 装置が再起動したときに通知を送信します。

linkdown: ポートのリンクがダウンしたときに通知を送信します。

linkup: ポートのリンクがアップしたときに通知を送信します。

warmstart: SNMP エージェントが再起動したときに通知を送信します。

system: システム時間が変更された、システムが再起動した、あるいはメインのシステムソフトウェアイメージが有効でないときに system 通知を指定します。

説明

snmp-agent trap enable コマンドはグローバルで SNMP 通知を有効にします。

undo snmp-agent trap enable コマンドはグローバルで SNMP 通知を無効にします。

プロトコル モジュールの SNMP トラップ機能については、このコマンドを正常に設定する前に、関連するプロトコルを有効にする必要があります。

IPv6 環境で SNMP トラップ機能を使用する場合は、SNMP のバージョン番号を v2c または v3 に設定してください。

指定したプロトコルモジュールのトラップ機能を有効にすると、モジュールはトラップ情報を生成して、モジュールの重要なイベントを通知します。生成されたトラップ情報は、デバイスの SNMP モジュールに送信されます SNMP でトラップ情報の送信パラメータを設定することにより、トラップ情報出力の関連する属性が決定されます。

オプションパラメータが指定されていない場合、すべてのオプションモジュールのトラップ機能がグローバルに有効または無効になります。

例

#SNMP 認証失敗のパケット機能を有効にします。

<Sysname> system-view

[Sysname] snmp-agent trap enable standard authentication

関連コマンド

- snmp-agent target-host
- snmp-agent sys-info version

4.1.30 snmp-agent trap if-mib link extended

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

デフォルト

SNMP エージェントは標準 linkUp/linkDown 通知を送信します。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap if-mib link extended コマンドは拡張 linkUp/linkDown 通知を送信するように SNMP エージェントを設定します。

undo snmp-agent trap if-mib link extended コマンドはデフォルトに戻します。

拡張 linkUp/linkDown 通知は、早急に故障個所を識別するため、標準 linkUp/linkDown 通知にインターフェースの説明とインターフェースのタイプを追加します。

このコマンドを使用するとき、NMS が拡張 linkUp/linkDown 通知をサポートしていることを確認してください。

例

拡張 linkUp/linkDown 通知を送信するように SNMP エージェントを設定します。

<AC> system-view

[AC] snmp-agent trap if-mib link extended

4.1.31 snmp-agent trap life

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

デフォルト

120 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

seconds: ライフタイムを指定します。設定範囲は 1～2592000 秒です。

説明

snmp-agent trap life コマンドは SNMP 通知キューの通知のライフタイムを設定します。

undo snmp-agent trap life コマンドはデフォルトの通知のライフタイムに戻します。

衝突が発生すると SNMP エージェントはキューに通知をバッファします。通知のライフタイムはキューに保持しておく期間を設定します。ライフタイムが終了したとき notification は削除されます。

例

SNMP 通知のライフタイムを 60 秒に設定します。

<AC> system-view

[AC] snmp-agent trap life 60

関連コマンド

- snmp-agent trap enable
- snmp-agent target-host
- snmp-agent trap queue-size

4.1.32 snmp-agent trap log

Syntax

snmp-agent trap log

undo snmp-agent trap log

デフォルト

無効

View

System view

定義済みユーザロール

network-admi

説明

snmp-agent trap log コマンドは SNMP 通知のロギングを有効にします。

undo snmp-agent trap log コマンドは SNMP 通知のロギングを無効にします。

通知のトラッキングを行うため、SNMP エージェントによって送信された SNMP 通知を記録するため、SNMP 通知のロギングを使用します。SNMP エージェントは Information Center にログを送信します。必要に応じて宛先にログを出力するように Information Center を設定することができます。

例

#SNMP アラームログ機能を有効にします。

<Sysname> system-view

[Sysname] snmp-agent trap log

4.1.33 snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

デフォルト

100

View

System view

定義済みユーザロール

network-admin

パラメータ

size: SNMP 通知のキューが保持できる通知の最大数を指定します。設定範囲は 1～1000 です。

説明

snmp-agent trap queue-size コマンドは SNMP 通知のキューのサイズを設定します。

undo snmp-agent trap queue-size コマンドはデフォルトのキューのサイズに戻します。

衝突が発生したとき、SNMP エージェントはキューに通知をバッファします。SNMP 通知のキューのサイズは SNMP 通知のキューが保持できる通知の最大数を設定します。キューのサイズが上限に到達したとき、新しい通知のために、古い通知が廃棄されます。

ユーザがキューの長さを変更した結果、キュー内の通知の数が送信キューの長さを超えると、古いアラーム情報は破棄されます。

例

SNMP 通知のキューのサイズを 200 に設定します。

<AC> system-view

[AC] snmp-agent trap queue-size 200

関連コマンド

- snmp-agent trap enable
- snmp-agent target-host
- snmp-agent trap life

4.1.34 snmp-agent usm-user { v1 | v2c }

Syntax

snmp-agent usm-user {**v1**|**v2c**} *user-name group-name* [**acl** {*ipv4-acl-number* |**name** *ipv4-acl-name* }]*

undo snmp-agent usm-user {**v1**|**v2c**} *user-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

user-name: SNMP ユーザ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

group-name: SNMPv1 あるいは SNMPv2c のグループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。グループは、すでに作成されたものでも指定できます。グループが作成されていない場合、グループを作成した後、適用されます。

acl:ユーザ名を標準または拡張 IPv4 ACL に指定します。

ipv4-acl-number:標準または拡張 IPv4 ACL 番号。ここで、標準 IPv4 ACL は 2000~2999 の値を取り、拡張 IPv4 ACL は 3000~3999 の値を取ります。

name *ipv4-acl-name*:標準または拡張 IPv4 ACL 名。1~63 文字の文字列で、大文字と小文字は区別されません。

説明

snmp-agent usm-user { **v1** | **v2c** }コマンドは SNMPv1 あるいは SNMPv2c グループにユーザを追加します。

undo snmp-agent usm-user { **v1** | **v2c** }コマンドは SNMPv1 あるいは SNMPv2c グループからユーザを削除します。

このコマンドを実行できるのは、network-admin または level-15 のユーザロールを持つユーザのみです。

SNMPv1 あるいは SNMPv2c では NMS エージェントはコミュニティ名を使用して互いに認証します。SNMPv3 ではユーザ名を使用して互いに認証します。

以下のどちらかの方法を使用して SNMPv1 あるいは SNMPv2c コミュニティを作成することができます。

- snmp-agent community コマンドを実行します。
- SNMPv1 あるいは SNMPv2c ユーザ、ユーザに割り当てられるグループを作成するため、snmp-agent usm-user { v1 | v2c }コマンド、snmp-agent group { v1 | v2c } コマンドを実行します。システムは SNMPv1 あるいは SNMPv2c のユーザ名を使用して自動で SNMP コミュニティを作成します。

ユーザ、グループのために ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し、ACL にルールが存在する場合、ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細な説明と説明については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。

例

#SNMP グループ readCom に SNMPv2c ユーザ userv2c を作成します。

<Sysname> system-view

[Sysname] snmp-agent sys-info version v2c

[Sysname] snmp-agent group v2c readCom

[Sysname] snmp-agent usm-user v2c userv2c readCom

#SNMP グループ readCom に SNMPv2c ユーザ userv2c を作成し、IP アドレス 1.1.1.1 の NMS のみがそのユーザ名を使用して Agent にアクセスできるようにし、他の NMS がそのユーザ名を使用してアクセスできないようにします。

<Sysname> system-view

[Sysname] acl basic 2900

[Sysname-acl-ipv4-basic-2900] rule permit source 1.1.1.1 0.0.0.0

[Sysname-acl-ipv4-basic-2900] rule deny source any

[Sysname-acl-ipv4-basic-2900] quit

[Sysname] snmp-agent sys-info version v2c

[Sysname] snmp-agent group v2c readCom

[Sysname] snmp-agent usm-user v2c userv2c readCom acl 2900

#SNMP グループ readCom に SNMPv2c ユーザ userv2c を作成し、IP アドレス 1.1.1.2 の NMS のみがそのユーザ名を使用して Agent にアクセスできるようにし、他の NMS がそのユーザ名を使用してアクセスできないようにします。

[Sysname] acl basic name testacl

[Sysname-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0

[Sysname-acl-ipv4-basic-testacl] rule deny source any

[Sysname-acl-ipv4-basic-testacl] quit

[Sysname] snmp-agent sys-info version v2c

[Sysname] snmp-agent group v2c readCom

[Sysname] snmp-agent usm-user v2c userv2c readCom acl name testacl

関連コマンド

- snmp-agent group
- snmp-agent community
- display snmp-agent community

4.1.35 snmp-agent usm-user v3

Syntax

VACM 方式:

snmp-agent usm-user v3 *user-name group-name* [**remote** { *ipv4-address* }] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* } }

RBAC 方式:

snmp-agent usm-user v3 *user-name* **user-role** *role-name* [**remote** { *ipv4-address* }] [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **aes192** | **aes256** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* | **remote** { *ipv4-address* } }

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

user-name: SNMPv3 ユーザ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

group-name: SNMPv3 のグループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

user-role *role-name*：ユーザロール名。role-name は、大文字と小文字が区別される 1 ～ 63 文字の文字列です。

remote { *ipv4-address* | **ipv6** *ipv6-address* } : Inform 情報を受信する宛先ホストの IPv4 アドレスまたは IPv6 アドレスで、通常は NMS の IPv4 アドレスです。デバイスが SNMPv3 Inform パケットを宛先ホストに送信する必要がある場合、このパラメータを設定する必要があり、snmp-agent remote コマンドを使用して、宛先ホストの IPv4 アドレスをエンジン ID に指定する必要があります。

cipher: 暗号化された形式で認証キーと暗号化キーを指定します。キーは暗号化された形式のダイジェストに変換され、デバイスに保存されます。

simple: 認証キーと平文の暗号化キーを指定します。キーは暗号化された形式のダイジェストに変換され、デバイスに保存されます。

authentication-mode: 認証アルゴリズムを指定します。キーワードを指定しないと、システムは認証を実行しません。値は以下の通りです。

- **md5**: HMAC-MD5 認証アルゴリズムを指定します。
- **sha**: HMAC-SHA1 認証アルゴリズムを指定します。

auth-password: プレーンテキストまたは認証キーを指定します。大文字、小文字を区別します。

- プレーンテキストの設定範囲は 1～64 文字です。数字、大文字、小文字、記号を含む必要があります。

- キーの暗号テキストは snmp-agent calculate-password コマンドで計算されます。

privacy-mode: 暗号アルゴリズムを指定します。指定しない場合、暗号を行いません。

- 3des: 128 ビットのキーを使用して 3DES アルゴリズムを指定します。
- aes128: 128 ビットのキーを使用して AES アルゴリズムを指定します。
- aes192: 192 ビットのキーを使用して AES アルゴリズムを指定します。
- aes256:256 ビットのキーを使用して AES アルゴリズムを指定します。
- des56: 56 ビットのキーを使用して DES アルゴリズムを指定します。

priv-password: プレーンテキストまたは暗号キーを指定します。大文字、小文字を区別します。

- プレーンテキストの設定範囲は 1～64 文字です。数字、大文字、小文字、記号を含む必要があります。
- キーの暗号テキストは snmp-agent calculate-password コマンドで計算されます。

acl:ユーザ名を標準または拡張 IPv4 ACL に指定します。

ipv4-acl-number:標準または拡張 IPv4 ACL 番号。ここで、標準 IPv4 ACL は 2000~2999 の値を取り、拡張 IPv4 ACL は 3000~3999 の値を取ります。

name *ipv4-acl-name*: 標準 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

local: ローカル SNMP エンジンを指定します。デフォルトでは、SNMPv3 ユーザはローカル SNMP エンジンに関連付けられています。

engineid *engineid-string*: 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。ローカルエンジンの ID を変更した後、既存の SNMPv3 ユーザと暗号化されたキーは無効になります。無効なユーザ名を削除する場合、undo snmp-agent usm-user v3 コマンドでユーザ名にエンジン ID を指定してください。

再度設定を行う必要があります。

説明

snmp-agent usm-user v3 コマンドは SNMPv3 ユーザを作成します。

undo snmp-agent usm-user v3 コマンドは SNMPv3 グループからユーザを削除します。

このコマンドを実行できるのは、network-admin または level-15 のユーザロールを持つユーザのみです。

SNMPv3 ユーザを作成する場合、ユーザのアクセス権を制御するための構成方法が 2 つあります。

- VACM:VACM モードはグループに SNMPv3 ユーザを割り当てる前に SNMPv3 グループを作成する必要があります。そうでない場合、グループが作成されたのち、ユーザが適用されません。SNMP グループは複数のユーザを含むことができます。SNMP グループはユーザのグループの MIB view とセキュリティモデルを指定します。各ユーザの認証と暗号化アルゴリズムは作成されたときに指定されます。

- RBAC: RBAC を使用して構成された SNMP ユーザはユーザロールに依存します。ユーザの作成時には、**user-role** *role-name* パラメータを使用してユーザロールを指定します。ユーザロールは、SNMP ユーザがアクセスできる SNMP オブジェクトと操作タイプ(ルールによる限定)を定義します。

VACM および RBAC を使用して SNMP ユーザを構成する場合は、次の点に注意してください。

- SNMP ユーザを VACM 方式で設定すると、ユーザ名が同じ場合、このコマンドが複数回実行され、最後に実行されたコマンドが有効になります。
- RBAC を使用して SNMP ユーザを構成する場合、このコマンドを複数回使用して、すでに作成されている SNMPv3 ユーザにユーザロールを追加できます。追加のパラメータが構成されていない場合、追加の構成は変更されず、ユーザロールのみが追加されます。他のパラメータ(認証方式)も設定する場合は、ユーザロールを追加し、他の設定も変更します。

acl パラメータを使用して、SNMP グループとユーザを作成し、ACL で許可されている NMS のみがデバイスにアクセスできるように、不正な NMS アクセスを制限できます。グループまたはユーザを作成する場合、ACL は次のルールに従います。

- ACL が参照されていない場合、ACL が存在しない場合、または参照した ACL にルールが設定されていない場合すべての NMS がデバイスにアクセスできます。
- 参照した ACL でルールが設定されている場合、ルール内の許可された NMS のみがデバイスにアクセスでき、他の NMS はデバイスにアクセスできません。

ACL の詳細な説明と説明については、QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“*15 セキュリティ*”の”*1 章 ACL*”を参照してください。

例

SNMPv3 グループ testGroup にユーザ testUser を追加します。グループでプライバシーセキュリティモデルなしで認証を有効にします。ユーザの認証アルゴリズムを HMAC-SHA11、プレーンテキストで認証キーを 123456TESTplat&!に設定します。

<Sysname> system-view

[Sysname] snmp-agent group v3 testGroup authentication

[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTplat&!

NMS での設定:バージョン番号 SNMPv3、ユーザ名 testUser、認証アルゴリズム HMAC-SHA1、認証パスワード 123456 TESTplat&!デバイスのデフォルトビュー内の MIB オブジェクトにアクセスできるように接続します。

#VACM 方式:v 3 グループ testGroup にユーザ testUser を追加し、セキュリティレベルは認証と暗号化、認証アルゴリズムは HMAC-SHA1、暗号化アルゴリズムは AES、認証パスワードはプレーンテキスト 123456 TESTauth&!、暗号化パスワードはプレーンテキスト 123456 TESTencr&!に設定します。

<Sysname> system-view

[Sysname] snmp-agent group v3 testGroup privacy

[Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTauth&!privacy-mode aes128 123456TESTencr&!

NMS での設定:バージョン番号 SNMPv3、ユーザ名 testUser、認証アルゴリズム HMAC-SHA1、認証パスワード 123456 TESTauth&!、暗号化アルゴリズムは AES、暗号化パスワードは 123456 TESTencr&!デバイスのデフォルトビュー内の MIB オブジェクトにアクセスできるように接続します。

<Sysname> system-view

[Sysname] snmp-agent remote 10.1.1.1 engineid 123456789A

[Sysname] snmp-agent group v3 testGroup privacy

[Sysname] snmp-agent usm-user v 3 remoteUser testGroup remote 10.1.1.1 simple authentication-mode sha 123456TESTauth&!privacy-mode aes128

123456TESTencr&!

#RBAC 方式:新しい SNMPv3 ユーザ testUser を作成します。役割は network-operator、セキュリティレベルは認証のみ暗号化なし、認証アルゴリズムは HMAC-SHA1、認証パスワードはプレーンテキスト 123456 TESTplat&!に設定します。

<Sysname> system-view

[Sysname] snmp-agent usm-user v3 testUser user-role network-operator simple authentication-mode sha 123456TESTplat&!

NMS での設定:バージョン番号 SNMPv3、ユーザ名 testUser、認証アルゴリズム HMAC-SHA1、認証パスワード 123456 TESTplat&!の順にクリックして、デバイス上のすべての MIB オブジェクトを読み取り専用にします。

関連コマンド

- display snmp-agent usm-user
- snmp-agent group
- snmp-agent calculate-password
- snmp-agent remote

目次

このセクションのページは **17-x-x** です。

5 章 RMON 5-1
5.1 RMON 設定コマンド 5-1
5.1.1 display rmon alarm 5-1
5.1.2 display rmon event 5-2
5.1.3 display rmon eventlog 5-4
5.1.4 display rmon history 5-6
5.1.5 display rmon prialarm 5-9
5.1.6 display rmon statistics 5-11
5.1.7 rmon alarm 5-13
5.1.8 rmon event 5-15
5.1.9 rmon history 5-16
5.1.10 rmon prialarm 5-18
5.1.11 rmon statistics 5-21

5章 RMON

5.1 RMON設定コマンド

5.1.1 display rmon alarm

Syntax

display rmon alarm [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

*entry-numbe*r: RMON アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、RMON アラームテーブルのすべてのエントリを表示します。

説明

display rmon alarm コマンドは RMON アラームテーブルのエントリを表示します。

例

RMON アラームテーブルのすべてのエントリを表示します。

<AC> display rmon alarm

```
AlarmEntry 1 owned by user1 is VALID.
Sample type : absolute
Sampled variable : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
Sampling interval (in seconds) : 10
Rising threshold : 50(associated with event 1)
Falling threshold : 5(associated with event 2)
Alarm sent upon entry startup : risingOrFallingAlarm
Latest value : 0
```

表 5-1 コマンド出力

フィールド	説明
AlarmEntry entry-number owned by owner is status.	アラームエントリのオーナと状態です。 • entry-number—アラームエントリのインデックスです。 • owner—エントリオーナです。 • status—エントリ状態です。 • VALID−エントリが有効です。 • UNDERCREATION−エントリが無効です。 statusフィールドはCLIで設定できません。CLIから作成されたすべてのアラームエントリはデフォルトで有効です。 display rmon alarmコマンドは無効のエントリを表示することができますが、display current-configurationコマンドとdisplay thisコマンドは設定を表示しません。
Sample type	サンプルタイプです。 • absolute • delta
Sampled variable	モニタされる変数です。
Sampling interval	サンプルされるデータの間隔（単位は秒）です。
Rising threshold	アラームの増加方向のしきい値です。
associated with event	アラームに関連したイベントインデックスです。
Falling threshold	アラームの減少方向のしきい値です。
Alarm sent upon entry startup	最初のサンプリングで生成できるアラーム • risingAlarm • fallingAlarm • risingOrFallingAlarm 最初のサンプリングにアラームタイプを指定しないと、**risingOrFallingAlarm**が有効になります。
Latest value	最後に取得したサンプル値です。

関連コマンド

- romon alarm

5.1.2 display rmon event

Syntax

display rmon event [*entry-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

entry-number: イベントエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、すべてのイベントエントリを表示します。

説明

display rmon event コマンドは RMON イベントエントリを表示します。

- イベントインデックス
- イベントオーナ
- イベント説明
- イベントによって発生するアクション（たとえば、イベントをロギングします、あるいは SNMP 通知を送信します）
- イベントが発生した最後の時間（システムが起動してからの経過時間です。単位は秒です）

例

すべてのイベントエントリを表示します。

<AC> display rmon event

```
EventEntry 1 owned by user1 is VALID.
Description: N/A
Community: Security
Take the action log-trap when triggered, last triggered at 0days 00h:02m:27s
uptime.
```

表 5-2 コマンド出力

フィールド	説明
EventEntry entry-number owned by owner is status.	イベントエントリのオーナと状態です。 ● entry-number—イベントエントリのインデックスです。 ● owner—エントリオーナです。 ● status—エントリ状態です。 ● VALID−エントリが有効です。 ● UNDERCREATION−エントリが無効です。 statusフィールドはCLIで設定できません。CLIから作成されたすべてのイベントエントリはデフォルトで有効です。 display rmon eventコマンドは無効のエントリを表示することができますが、display current-configurationコマンドとdisplay thisコマンドは設定を表示しません。
Description	イベント説明です。
Community	RMONイベントのSNMPコミュニティ名です。
Take the action action when triggered	イベントが発生したときのアクションです。 ● none—アクションを行いません。 ● log—イベントをロギングします。 ● trap—SNMP通知を送信します。 ● log-trap—イベントをロギングし、SNMP通知を送信します。
last triggered at time uptime	イベントが発生したときの最後の時間です。システムが起動してからの経過時間として表示されます。

関連コマンド

- rmon event

5.1.3 display rmon eventlog

Syntax

display rmon eventlog [*entry-number*]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

entry-number: イベントエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、すべてのイベントエントリを表示します。

説明

display rmon eventlog コマンドはイベントログのエントリを表示します。

イベントのログのアクションが指定されている場合、イベントが発生する毎に、イベントログテーブルにレコードを追加します。各レコードはログエントリインデックス、イベントがログされた時間（システムが起動してからの経過時間）、イベント説明を含みます。

システムはイベントに 10 個のレコードを追加することができます。レコードが 10 になったとき、古いレコードを最新のレコードに置き換えます。

例

イベントエントリ 99 の RMON ログを表示します。

<AC> display rmon eventlog 99

```
EventEntry 99 owned by ww is VALID.
LogEntry 99.1 created at 50days 08h:54m:44s uptime.
Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
uprise 16760000 with alarm value 16776314. Alarm sample type is absolute.
LogEntry 99.2 created at 50days 09h:11m:13s uptime.
Description: The 1.3.6.1.2.1.16.1.1.1.4.5 defined in alarmEntry 77,
less than(or =) 20000000 with alarm value 16951648. Alarm sample type is
absolute.
LogEntry 99.3 created at 50days 09h:18m:43s uptime.
Description: The alarm formula defined in prialarmEntry 777,
less than(or =) 15000000 with alarm value 14026493. Alarm sample type is
absolute.
LogEntry 99.4 created at 50days 09h:23m:28s uptime.
Description: The alarm formula defined in prialarmEntry 777,
uprise 17000000 with alarm value 17077846. Alarm sample type is absolute.
```

上記の例は、イベント 99 によって生成されたアラームイベントログを示しており、アラームテーブルによって生成されたイベントログが 2 つ、拡張アラームテーブルによって生成されたイベントログが 2 つあります。

表 5-3 コマンド出力

フィールド	説明
EventEntry entry-number owned by owner is status.	イベントログエントリのオーナと状態です。 ● entry-number—イベントログエントリのインデックスです。ログエントリが作成されたイベントエントリのインデックスと同一です。 ● owner—エントリオーナです。 ● status—エントリ状態です。 ● VALID—エントリが有効です。（デフォルトです） ● UNDERCREATION—エントリが無効です。 statusフィールドはCLIで設定できません。CLIから作成されたすべてのイベントログエントリはデフォルトで有効です。 display rmon eventlogコマンドは無効のエントリを表示することができますが、display current-configurationコマンドとdisplay thisコマンドは設定を表示しません。
LogEntry entry-number created at created-time uptime.	イベントレコードが作成された時間です。 ● entry-number—イベントレコードインデックスです。logEventIndex.logIndexとして示されます。logEventIndexとlogIndexはMIBオブジェクトです。イベントのすべてのレコードのなかでレコードを一意に識別します。 ● created-time—イベントエントリが作成された時間です。
Description	レコードの説明です。

関連コマンド

- rmon event

5.1.4 display rmon history

Syntax

display rmon history [*interface-type interface-number*]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースを指定しない場合、RMON 履歴管理エントリがあるすべてのインタフェースの履歴サンプルを表示します。

説明

display rmon history コマンドは Ethernet インタフェースの RMON 履歴管理エントリと Ethernet 履歴のサンプルの統計情報を表示します。

RMON は Ethernet インタフェースの Ethernet 履歴のサンプルを記録するため、etherHistoryTable オブジェクトを使用します。

Ethernet インタフェースの履歴サンプルを収集するため、最初にインタフェースで履歴管理エントリを作成する必要があります。

表示できる履歴サンプルの数とサンプリング間隔を設定する場合、**rmon history** コマンドを使用します。

例

GigabitEthernet 1/0/1 の RMON 履歴管理エントリと履歴のサンプルの情報を表示します。

<AC> display rmon history gigabitethernet 1/0/1

```
HistoryControlEntry 6 owned by user1 is VALID.
Sampled interface:GigabitEthernet1/0/1 <ifIndex.117>
Sampling interval:8 (秒) with 3 buckets max
Sampling record 1 :
dropevents:0、octets:5869
packets:54、broadcast packets:9
multicast packets :23, CRC alignment errors :0
undersize packets :0、oversize packets:0
fragments:0、jabbers:0
collisions:0、utilization:0
```

表 5-4 コマンド出力

フィールド	説明
HistoryControlEntry entry-number owned by owner is status.	ヒストリ制御エントリのオーナと状態です。 ● entry-number—ヒストリ制御エントリのインデックスです。 ● owner—エントリオーナです。 ● status—エントリ状態です。 ● VALID–エントリが有効です。 ● UNDERCREATION–エントリが無効です。 statusフィールドはCLIで設定できません。CLIから作成されたすべてのヒストリ制御エントリはデフォルトで有効です。 The display rmon historyコマンドは無効のエントリを表示することができますが、display current-configurationコマンドとdisplay thisコマンドは設定を表示しません。
Sampled Interface	サンプルされるインタフェースです。
Sampling interval	サンプルされるデータの間隔です。単位は秒です。
buckets max	履歴管理エントリで保存できるサンプルの最大数です。 rmon historyコマンドで設定した、予期したバケットサイズが有効な履歴テーブルサイズを超過した場合、RMONはバケットサイズをできるだけ、予期したバケットサイズに近づけます。 バケットサイズが一杯になったとき、RMONは新しいサンプルを古いサンプルに上書きします。
Sampling record	履歴サンプルインデックスです。
dropevents	サンプリング間隔中にパケットが廃棄されたイベントの総数です。
octets	サンプリング間隔中に受信したオクテット数です。
packets	サンプリング間隔中に受信したパケットの総数（不良パケットを含みます）です。
broadcast packets	サンプリング間隔中に受信したブロードキャストパケットの総数です。
multicast packets	サンプリング間隔中に受信したマルチキャストパケットの総数です。
CRC alignment errors	サンプリング間隔中に受信したCRCエラーパケットの数です。
undersize packets	サンプリング間隔中に受信した過小サイズのエラーパケットの数です。 過小サイズエラーパケットはパケット長が64オクテット未満のパケットです。（フレームビットを除き、FCSオクテットを含みます）

フィールド	説明
oversize packets	サンプリング間隔中に受信した過大サイズのエラーパケットの数です。 過大サイズエラーパケットはパケット長が1518オクテットより長いパケットです。（フレームビットを除き、FCSオクテットを含みます）
fragments	サンプリング間隔中に受信した過小サイズのCRCエラーパケットの数です。
jabbers	サンプリング間隔中に受信した過大サイズのCRCエラーパケットの数です。
collisions	サンプリング間隔中に受信したコリジョンパケットの数です。
utilization	サンプリング間隔中の帯域幅の使用率です。（単位は%です）

関連コマンド

- rmon history

5.1.5 display rmon prialarm

Syntax

display rmon prialarm [*entry-number*]

View

すべての view

定義済みユーザーロール

network-admin

netwoek-operator

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。指定しない場合、すべてのプライベートアラームエントリを表示します。

説明

display rmon prialarm コマンドはプライベート RMON アラームテーブルのエントリを表示します。

例

すべてのプライベートアラームエントリを表示します。

<AC> display rmon prialarm

```
PrialarmEntry 1 owned by user1 is VALID.
Sample type: absolute
```

```
Variable formula:(.1.3.6.1.2.1.16.1.1.6 .1*100/.1.3.6.1.2.1.16.1.1.5 .1)
Description : if Utilization.GigabitEthernet1/0/1
Sampling interval (in seconds):10
Rising threshold:80 (associated with event 1)
Falling threshold:5 (associated with event 2)
Alarm sent upon entry startup: rising Or FallingAlarm
Entry life time : forever
Latest value:85
```

表 5-5 コマンド出力

フィールド	説明する
PrialarmEntry entry-number owned by owner is status.	プライベートアラームエントリのオーナと状態です。 ● entry-number—プライベートアラームエントリのインデックスです。 ● owner—エントリオーナです。 ● status—エントリ状態です。 ● VALID–エントリが有効です。 ● UNDERCREATION–エントリが無効です。 statusフィールドはCLIで設定できません。CLIから作成されたすべてのプライベートアラームエントリはデフォルトで有効です。display rmon prialarmコマンドは無効のエントリを表示することができますが、display current-configurationコマンドとdisplay thisコマンドは設定を表示しません。
Sample type	サンプルタイプです。 ● absolute ● delta
Variable formula	変数の式です。
Description	アラームエントリの説明です。
Sampling interval	サンプルされるデータの間隔です。単位は秒です。
Rising threshold	アラームの増加方向のしきい値です。
Falling threshold	アラームの減少方向のしきい値です。
associated with event	アラームに関連したイベントインデックスです。
Alarm sent upon entry startup	最初のサンプリングで生成できるアラーム ● risingAlarm ● fallingAlarm ● risingOrFallingAlarm 最初のサンプリングにアラームタイプを指定しないと、**risingOrFallingAlarm**が有効になります。

フィールド	説明する
Entry lifetime	エントリの有効期限です。 ● 有効期限がforeverに設定されている場合、エントリは削除されません。 ● 有効期限に時間が設定されている場合、時間が終了したときエントリが削除されます。
Latest value	最後に取得したサンプル値

関連コマンド

- rmon prilarm

5.1.6 display rmon statistics

Syntax

display rmon statistics [*interface-type interface-number*]

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。インタフェースを指定しない場合、すべてのインタフェースの RMON の統計情報を表示します。

説明

display rmon statistics コマンドは RMON の統計情報を表示します。

このコマンドは、統計情報エントリが作成された時間からコマンドが実行された時間までの期間のインタフェース統計情報を表示します。装置が再起動するとその統計情報は削除されます。

例

GigabitEthernet 1/0/1 の RMON の統計情報を表示します。

<AC> display rmon statistics gigabitethernet 1/0/1

```
EtherStatsEntry 1 owned by user1 is VALID.
Interface :GigabitEthernet1/0/1 <ifIndex.3>
etherStatsOctets:43393306、etherStatsPkts:619825
etherStatsBroadcastPkts:503581, etherStatsMulticastPkts :44013
etherStatsUndersizePkts:0、etherStatsOversizePkts:0
```

```
etherStatsFragments:0、etherStatsJabbers:0
etherStatsCRCAlignErrors :0、etherStatsCollisions:0
etherStatsDropEvents (insufficient resources):0
Incoming packets by size:
64:0, 65-127:0, 128-255:0
256-511:0, 512-1023:0, 1024-1518:0
```

表 5-6 コマンド出力

フィールド	説明
EtherStatsEntry entry-number owned by owner is status.	統計情報エントリのオーナと状態です。 ● entry-number—統計情報エントリのインデックスで ● owner—エントリオーナです。 ● status—エントリ状態です。 ● VALID—エントリが有効です。 ● UNDERCREATION—エントリが無効です。 statusフィールドはCLIで設定できません。CLIから作成されたすべての統計情報エントリはデフォルトで有効です。display rmon statisticsコマンドは無効のエントリを表示することができますが、display current-configurationコマンドとdisplay thisコマンドは設定を表示しません。
Interface	統計情報が収集されたインタフェースです。
etherStatsOctets	インタフェースで受信したオクテットの総数です。
etherStatsPkts	インタフェースで受信したパケットの総数です。
etherStatsBroadcastPkts	インタフェースで受信したブロードキャストパケットの総数です。
etherStatsMulticastPkts	インタフェースで受信したマルチキャストパケットの総数です。
etherStatsUndersizePkts	インタフェースで受信した過小サイズのエラーパケットの総数です。
etherStatsOversizePkts	インタフェースで受信した過大サイズのエラーパケットの総数です。
etherStatsFragments	統計時間中にポートが受信したすべての過小検査エラーパケットの数
etherStatsJabbers	インタフェースで受信した過大サイズのCRCエラーパケットの総数です。
etherStatsCRCAlignErrors	インタフェースで受信したCRCエラーパケットの総数です。
etherStatsCollisions	インタフェースで受信したコリジョンパケットの総数です。
etherStatsDropEvents	廃棄されたパケットのイベント総数です。

フィールド	説明
Incoming packets by size:	パケット長毎の入力パケットです。 • 64—長さが64バイト以下のパケット数。 • 65-127—65～127バイト長のパケット数です。 • 128-255—128～255バイト長のパケット数です。 • 256-511—256～511バイト長のパケット数です。 • 512-1023—512～1023バイト長のパケット数です。 • 1024-1518—1024～1518バイト長のパケット数です。

関連コマンド

- rmon statistics

5.1.7 rmon alarm

Syntax

rmon alarm *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

デフォルト

設定なし

View

System view

定義済みユーザーロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

alarm-variable: アラーム変数を指定します。設定範囲は 1～255 です。変数は ASN.1 INTEGER（INTEGER、NTEGER32、Unsigned32、Counter32、Counter64、Gauge、TimeTicks）のみを使用できます。アラーム変数は表 5-7 の 1 つを使用します。

sampling-interval: サンプリング間隔を指定します。設定範囲は 5～65535 秒です。

absolute: 絶対値のサンプリングを指定します。RMON はサンプリング間隔の両端で増加方向のしきい値と減少方向のしきい値を比較します。

delta: 相対値のサンプリングを指定します。RMON は現在の値から前に取得したサンプル値を引き、増加方向と減少方向のしきい値の差異を比較します。

startup-alarm: アラームエントリが有効なときに作成されるアラームを指定します。アラームを指定しない場合、RMON は最初のサンプルに依存して増加方向のアラームあるいは減少方向のアラームを作成します。

rising: エントリが有効になったのち、最初にサンプルが増加方向のしきい値以上になった場合に、増加方向のアラームを作成します。

falling: エントリが有効になったのち、最初にサンプルが減少方向のしきい値以下になった場合に、減少方向のアラームを作成します。

rising-falling: 最初のサンプルが増加方向のしきい値と交差した場合、増加方向のアラームを作成します。あるいは最初のサンプルが減少方向のしきい値と交差した場合、減少方向のアラームを作成します。

rising-threshold *threshold-value1 event-entry1*: 増加方向のしきい値を指定します。*threshold-value1* の設定範囲は-2147483648 ～ +2147483647 です。*event-entry1* は増加方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry1* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

falling-threshold *threshold-value2 event-entry2*: 減少方向のしきい値を指定します。threshold-value2 の設定範囲は-2147483648 ～ +2147483647 です。*event-entry2* は減少方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry2* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon alarm コマンドは RMON アラームテーブルのエントリを作成します。

undo rmon alarm コマンドは RMON アラームテーブルからエントリを削除します。

RMON アラームテーブルに最大 60 のエントリを作成することができます。

アラームエントリは固有のアラーム変数、サンプリング間隔、サンプリングタイプ、増加方向のしきい値あるいは減少方向のしきい値がある必要があります。エントリのすべてのパラメータが既存のエントリと同一である場合、アラームエントリを作成することができません。

アラーム状況に関連したイベントを発生させるため、**rmon event** コマンドでイベントを作成する必要があります。

RMON は指定されたサンプリング間隔でモニタ対象のアラーム変数をサンプリングします。予期されたしきい値とサンプリングされた値と比較し、以下の 1 つの処理を行います。

- サンプリングした値が増加方向のしきい値以上である場合、増加方向のアラームに関連したイベントを発生します。
- サンプリングした値が減少方向のしきい値以下である場合、減少方向のアラームに関連したイベントを発生します。

例

GigabitEthernet 1/0/1 でアラームテーブルにエントリ 1 を作成します。サンプリングタイプを absolute （絶対値）にし、オブジェクト ID 1.3.6.1.2.1.16.1.1.1.4.1 を 10 秒間隔でサンプリングします。サンプリングした値が上昇しきい値 5000 以上になった場合、増加方向のアラームイベントをロギングします。サンプリングした値が 5 以下である場合、アクションは発生しません。

<AC> system-view

[AC] rmon event 1 log

[AC] rmon event 2 none

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] rmon statistics 1

[AC-GigabitEthernet1/0/1] quit

[AC] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising-threshold 5000 1 falling-threshold 5 2 owner user1

この例では、1.3.6.1.2.1.16.1.1.1.4.1 を etherStatsOctets に置き換えることができます。ここで 1 はインタフェースのエントリインデックスの統計情報です。rmon statistics 5 コマンドを実行した場合、1.3.6.1.2.1.16.1.1.1.4.5 を置き換えるために etherStatsOctets を使用します。

関連コマンド

- display rmon alarm
- rmon event

5.1.8 rmon event

Syntax

rmon event *entry-number* [**description** *string*] { **log** | **log-trap** *security-string* | **none** | **trap** *security-string* } [**owner** *text*]

undo rmon event *entry-number*

デフォルト

設定なし

View

System-view

定義済みユーザーロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

description *string*: イベントの説明を設定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

log: イベントが発生したとき、ログを取得します。

log-trap: イベントが発生したとき、ログを取得し、SNMP 通知を送信します。

security-string: SNMP コミュニティを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。SNMP の設定に依存します。このパラメータは現在のソフトウェアバージョンでサポートしていません。

none: イベントが発生したとき、アクションを行いません。

trap: イベントが発生したとき、SNMP 通知を送信します。

owner text: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon event コマンドは RMON イベントテーブルのエントリを作成します。

undo rmon event コマンドは RMON イベントテーブルからエントリを削除します。

最大 60 のイベントエントリを作成することができます。

アラーム状況が発生したとき、アクションを指定するため、イベントエントリを標準あるいはプライベートアラームエントリに関連づけることができます。設定に依存して、イベントのログを取得し、SNMP 通知を送信することができます。

1 つのイベントを複数のアラームエントリに関連づけることができます。

例

RMON イベントエントリを作成します。イベント 10、エントリオーナ user1 を指定します。

<AC> system-view

[AC] rmon event 10 log owner user1

関連コマンド

- display rmon event
- rmon alarm
- rmon prialarm

5.1.9 rmon history

Syntax

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]

undo rmon history *entry-number*

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザーロール

network-admin

パラメータ

entry-number: 履歴管理エントリのインデックスを指定します。設定範囲は 1～65535 です。

buckets *number*: エントリのために記録されるサンプルの予期する最大数を指定します。設定範囲は 1～65535 です。RMON は各履歴管理エントリで 50 のサンプルを記録することができます。予期したバケットサイズが有効な履歴テーブルサイズを超過した場合、RMON はバケットサイズをできるだけ、予期したバケットサイズに近づけます。しかし 50 を超過することはできません。たとえば、予期したバケットサイズを 55 に設定し、有効なバケットサイズが 30 である場合、履歴管理エントリのバケットサイズは 30 となります。

interval *sampling-interval*: サンプリング間隔を指定します。設定範囲は 5～3600 秒です。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon history コマンドは RMON 履歴管理テーブルのエントリを作成します。

undo rmon history コマンドは RMON 履歴管理テーブルからエントリを削除します。

レイヤ 2 Ethernet インタフェースあるいはレイヤ 3 Ethernet インタフェースでのみ RMON 履歴管理エントリを作成することができます。

システムで最大 100 の履歴管理エントリを作成することができます。

Ethernet インタフェースで履歴管理エントリがある場合、RMON はインタフェースで定期的にパケットの統計情報をサンプリングし、履歴テーブルにサンプルを記録します。履歴管理エントリのバケットサイズが最大になったとき、RMON は古いサンプルを新しいサンプルに上書きします。

1 つのインタフェースで複数の履歴管理エントリを設定することができますが、エントリ数とサンプリング間隔を変更する必要があります。

例

GigabitEthernet 1/0/1 で RMON 履歴管理テーブルのエントリ 1 を作成します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] rmon history 1 buckets 10 interval 5 owner user1

関連コマンド

- dispalay rmon history

5.1.10 rmon prialarm

Syntax

rmon prialarm entry-number *prialarm-formula prialarm-des sampling-interval* { **absolute** | **delta** } [**startup-alarm** { **falling** | **rising** | **rising-falling** }] **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]

undo rmon prialarm *entry-number*

デフォルト

設定なし

View

System-view

定義済みユーザーロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

prialarm-formula: プライベートアラーム変数を指定します。設定範囲は 1～255 文字です。変数の式はドット（.）始まる OID で示されます。たとえば、(.1.3.6.1.2.1.2.1.10.1) *8 です。この変数は、加減乗除の四則演算を行うことができます。演算の結果は長整数になります。エラーを防ぐため、演算の各段階の結果が、以下の値になるようにしてください。

- 式の変数の値が整数
- 設定範囲各計算のステップが long 整数

prialarm-des: エントリの説明を設定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

sampling-interval: サンプリング間隔を指定します。設定範囲は 10～65535 秒です。

absolute: 絶対値のサンプリングを指定します。RMON はサンプリング間隔の両端で増加方向のしきい値と減少方向のしきい値を比較します。

delta: 相対値のサンプリングを指定します。RMON は現在の値から前に取得したサンプル値を引き、増加方向と減少方向のしきい値の差異を比較します。

startup-alarm: アラームエントリが有効なときに作成されるアラームを指定します。アラームを指定しない場合、RMON は以下を行います。

- 最初のサンプルが増加方向のしきい値を交差したとき、増加方向のアラームを作成します。
- 最初のサンプルが減少方向のしきい値を交差したとき、減少方向のアラームを作成します。

rising: エントリが有効になったのち、最初にサンプルが増加方向のしきい値以上になった場合に、増加方向のアラームを作成します。

falling: エントリが有効になったのち、最初にサンプルが減少方向のしきい値以下になった場合に、減少方向のアラームを作成します。

rising-falling: 最初のサンプルが増加方向のしきい値と交差した場合、増加方向のアラームを作成します。あるいは最初のサンプルが減少方向のしきい値と交差した場合、減少方向のアラームを作成します。

rising-threshold *threshold-value1 event-entry1*: 増加方向のしきい値を指定します。*threshold-value1* の設定範囲は-2147483648 ～ +2147483647 です。*event-entry1* は増加方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry1* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

falling-threshold *threshold-value2 event-entry2*: 減少方向のしきい値を指定します。threshold-value2 の設定範囲は-2147483648 ～ +2147483647 です。*event-entry2* は減少方向のしきい値が交差したとき発生するイベントのインデックスを示します。*event-entry2* の設定範囲は 0～65535 です。0 が指定された場合、イベントでアラームが発生しません。

forever: 無期限のエントリを指定します。RMON は手動で削除するまで無期限のプライベートアラームエントリを保持します。

cycle *cycle-period*: エントリの有効期限を指定します。設定範囲は 0～4294967 秒です。RMON は有効期限が終了したとき、エントリを削除します。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon prialarm コマンドはプライベートアラームテーブルのエントリを作成します。

undo rmon prialarm コマンドはプライベートアラームテーブルからエントリを削除します。

最大 50 のプライベートアラームエントリを作成することができます。

アラームエントリは固有のアラーム変数、サンプリング間隔、サンプリングタイプ、増加方向のしきい値あるいは減少方向のしきい値がある必要があります。エントリのすべてのパラメータが既存のエントリと同一である場合、アラームエントリを作成することができません。

アラーム状況に関連したイベントを発生させるため、**rmon event** コマンドでイベントを作成する必要があります。

RMON エージェントは変数をサンプリングし、プライベートアラームエントリをもとにしてアラームのアクションを行います。

1) プライベートアラームの式で指定された変数を定期的にサンプリングします。
2) 式でサンプリングした値を処理します。
3) 計算結果と予期されたしきい値を比較し、以下のアクションの 1 つを行います。

- 結果が増加方向のしきい値以上である場合、増加方向のアラームに関連したイベントを発生します。
- 結果が減少方向のしきい値以下である場合、減少方向のアラームに関連したイベントを発生します。

例

GigabitEthernet 1/0/1 で入力パケットの総数と入力ブロードキャストの割合をモニタするため、無期限のプライベートアラームエントリを追加します。割合が 80%を超過したとき、増加方向のアラームイベントのログを取得し、割合が 5%以下になったとき、アクションを行いません。式は（1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1）です。ここで 1.3.6.1.2.1.16.1.1.1.6.1 はオブジェクトインスタンス etherStatsBroadcastPkts.1 の OID です。1.3.6.1.2.1.16.1.1.1.5.1 はオブジェクトインスタンス etherStatsPkts.1 の OID です。

<AC> system-view

[AC] rmon event 1 log

[AC] rmon event 2 none

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] rmon statistics 1

[AC-GigabitEthernet1/0/1] quit

[AC]rmon prialarm 1 (.1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1) BroadcastPktsRatioOfEth1/1 10 absolute rising-threshold 80 1 falling-threshold 5 2 entrytype forever owner user1

変数の OID の最後の数はインタフェースのエントリインデックスの統計情報と同一にする必要があります。たとえば、rmon statistics 5 コマンドを実行するとき、それぞれ 1.3.6.1.2.1.16.1.1.1.6.1 、 1.3.6.1.2.1.16.1.1.1.5.1 を 1.3.6.1.2.1.16.1.1.1.6.5 、1.3.6.1.2.1.16.1.1.1.5.5 に置き換えます。

関連コマンド

- display rmon prialarm
- rmon event

5.1.11 rmon statistics

Syntax

rmon statistics *entry-number* **[owner** *text*]

undo rmon statistics *entry-number*

デフォルト

設定なし

View

Ethernet interface view

定義済みユーザーロール

network-admin

パラメータ

entry-number: アラームエントリのインデックスを指定します。設定範囲は 1～65535 です。

owner *text*: エントリオーナを指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rmon statistics コマンドは RMON 統計情報テーブルのエントリを作成します。

undo rmon statistics コマンドは RMON 統計情報テーブルからエントリを削除します。

レイヤ 2 Ethernet インタフェースあるいはレイヤ 3 Ethernet インタフェースでのみ RMON 統計情報エントリを作成することができます。

各インタフェースで 1 つの統計情報のエントリを作成することができます。

装置で最大 100 の統計情報エントリを作成することができます。

各 RMON 統計情報テーブルエントリは、インタフェースで収集したトラフィックを現在の時間まで累積した統計情報の合計です。統計情報はコリジョン、過大サイズの CRC エラーパケットの数、過大サイズのパケット数、過小サイズのパケット数、ブロードキャストパケット数、マルチキャストパケット数、受信したバイト数、受信したパケット数を含みます。統計情報は、再起動で削除されます。

RMON 統計情報のテーブルを表示する場合、**display rmon statistics** コマンドを使用します。

例

GigabitEthernet 1/0/1 でインデックス 20、オーナ user1 の RMON 統計情報エントリを作成します。

<AC> system-view

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] rmon statistics 20 owner user1

関連コマンド

- display rmon statistics

目次

このセクションのページは **17-x-x** です。

6 章 NETCONF 6-1
6.1 NETCONF 設定コマンド 6-1
6.1.1 netconf log 6-1
6.1.2 netconf soap enable 6-3
6.1.3 netconf soap http port 6-3
6.1.4 netconf ssh server enable 6-4
6.1.5 xml 6-5

6章 NETCONF

6.1 NETCONF設定コマンド

6.1.1 netconf log

Syntax

netconf log source { **all** | { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **row-operation** | **verbose** }

undo netconf log source { **all** | { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **row-operation** | **verbose** }

デフォルト

無効

View

System-view

定義済みユーザーロール

network-admin

パラメータ

source:プロトコルを使用するクライアントを表す NETCONF オペレーションソースを指定します。

- **all**:すべてのプロトコルを使用する NETCONF クライアントを指定します。
- **agent**:Telnet、SSH、NETCONF over console、NETCONF over Telnet、または NETCONF over SSH を使用するクライアントを指定します。
- **soap**:SOAP over HTTP または SOAP over HTTPS を使用するクライアントを指定します。
- **web**:Web を使用するクライアントを指定します。
- **protocol-operation**:特定の種類の NETCONF 操作の要求と応答をログに記録します。
- **all**:すべてのタイプの NETCONF 操作を指定します。
- **action**:<action>動作を指定します。
- **config**:<CLI>、<save>、<load>、<rollback>、<lock>、<unlock>、<save-point>操作など、設定関連の NETCONF 操作を指定します。
- **get**:<get>、<get-config>、<get-bulk>、<get-bulk-config>、および<get-sessions>操作を含む、データ取得関連の NETCONF 操作を指定します。
- **session**:<kill-session> および <close-session> 操作を含むセッション関連の NETCONF 操作、および hello メッセージによる機能交換を指定します。

- **set**:すべての<edit-config>操作を指定します。
- **syntax**:XML およびスキーマエラーを含む要求を指定します。
- **others**:キーワード action、config、get、set、session、および syntax で指定された操作以外の NETCONF 操作を指定します。

row-operation:<action>および<edit-config>操作の行操作をログに記録します。

verbose:形式が正しい要求のパケットの内容や失敗した<edit-config>操作に関するエラー情報など、NETCONF 操作の種類に関する要求と応答の詳細情報をログに記録します。

説明

netconf log コマンドは、NETCONF ログ機能を有効にします。

undo netconf log コマンドは、NETCONF ログ機能を無効にします。

NETCONF ログ機能では、NETCONF 操作タイプ(protocol-operation)でログを出力し、NETCONF 行(row-operation)でログを出力できます。

- NETCON オペレーションタイプ別にログを出力するように設定すると、ユーザが NETCONF オペレーションを実行するたびに、デバイスは NETCONF オペレーションのログとオペレーション結果を出力します。たとえば、ユーザが NETCONF オペレーションを実行して ID 3~5 の VLAN を作成すると、デバイスは次のログを出力します。

```
%Mar 21 17:11:34:479 2019 Sysname XMLSOAP/6/XML_REQUEST:test from 192.168.100.198, session id 2, message-id 100, receive edit-config request.
%Mar 21 17:11:34:483 2019 Sysname XMLSOAP/6/EDIT-CONFIG:test from 192.168.100.198, session id 2, message-id 100, execute success.
```

- NETCONF 行でログを出力するように設定されている場合、ユーザが NETCONF オペレーションを実行すると、デバイスはそのオペレーションの各要求行のログを出力します。たとえば、ユーザが NETCONF オペレーションを実行して ID 3~5 の VLAN を作成すると、デバイスは次のログを出力します。

```
%Mar 31 17:50:02:608 2019 Sysname XMLSOAP/6/EDIT-CONFIG:User (test, 192.168.100.20, session ID 1)、 message ID=100, operation=create VLAN/VLANs (ID=3)、 result=Succeeded.No attributes.
%Mar 31 17:50:02:609 2019 Sysname XMLSOAP/6/EDIT-CONFIG:User (test, 192.168.100.20, session ID 1)、 message ID=100, operation=create VLAN/VLANs (ID=4)、 result=Succeeded.No attributes.
%Mar 31 17:50:02:611 2019 Sysname XMLSOAP/6/EDIT-CONFIG:User (test, 192.168.100.20, session ID 1)、 message ID=100, operation=create VLAN/VLANs (ID=5)、 result=Succeeded.No attributes.
```

デバイスはまず NETCONF ログを情報センターに送信し、情報センターの出力規則に従って異なる方向にログ情報を出力します。

例

#設定デバイスは、agent から edit-config タイプの操作ログを出力します。

<Sysname> system-view

[sysname] netconf log source agent protocol-operation set

6.1.2 netconf soap enable

Syntax

netconf soap { **http** | **https** } **enable**

undo netconf soap { **http** | **https** } **enable**

デフォルト

無効

View

System-view

定義済みユーザーロール

network-admin

パラメータ

http : HTTP ベースの NETCONF over SOAP 機能を有効にします。

https : HTTPS ベースの NETCONF over SOAP 機能を有効にします。

説明

netconf soap enable コマンドは、NETCONF over SOAP 機能を有効にします。

undo netconf soap enable コマンドは、NETCONF over SOAP 機能を無効にします。

このコマンドを設定すると、デバイスはそのような HTTP/HTTPS パケットを解析できるようになり、パケット内のデータは SOAP カプセル化された NETCONF コマンドになります。

例

SOAP over HTTP 機能を有効にします。

<Sysname> system-view

[Sysname] netconf soap http enable

6.1.3 netconf soap http port

Syntax

netconf soap http port *port-number*

undo netconf soap http port

デフォルト

80

View

System view

定義済みユーザーロール

network-admin

パラメータ

port-number: ポート番号を 1 から 65535 の範囲で指定します。

説明

NETCONF over SOAP over HTTP セッションに使用するポートを指定するには、**netconf soap http port** コマンドを使用します。

デフォルトに戻すには、**undo netconf soap http port** コマンドを使用します。

このコマンドを実行すると、既存のッションが無効になります。セッションを再度確立する必要があります。

例

NETCONF over SOAP over HTTP セッションにポート 1000 を使用します。

<Sysname> system-view

[Sysname] netconf soap http port 1000

6.1.4 netconf ssh server enable

Syntax

netconf ssh server enable

undo netconf ssh server enable

デフォルト

無効

View

System view

定義済みユーザーロール

network-admin

説明

SSH 経由の NETCONF を有効にするには、**netconf ssh server enable** コマンドを使用します。

SSH 経由の NETCONF を無効にするには、**undo netconf ssh server enable** コマンドを使用します。

この機能を使用すると、SSH クライアントを使用して SSH サブシステムとして NETCONF を呼び出すことができます。その後、xml コマンドを使用せずに XML メッセージを直接使用して NETCONF 操作を実行できます。

このコマンドを実行する前に、デバイスでユーザの認証モードを **scheme** として設定します。これにより、NETCONF over SSH 対応のユーザ端末は、NETCONF over SSH 経由でデバイスにアクセスできるようになります。

capability は **urn:ietf:params:netconf:base:1.0** のみが使用可能です。デバイスとユーザ端末の両方でサポートされます。

例

NETCONF over SSH を有効にします。

<Sysname> system-view

[Sysname] netconf ssh server enable

6.1.5 xml

Syntax

xml

View

User-view

定義済みユーザーロール

network-admin

network-operator

説明

xml コマンドを使用して XML ビューにアクセスします。

XML ビューに移動すると、NETCONF コマンドを入力してシステムデータを設定または取得できます。ユーザがログインするときに使用する役割によって、実行できる NETCONF オペレーションは異なります。

- network-admin:すべてのオペレーションを実行できます。
- network-operator :get、get-bulk、get-config、get-bulk-config、get-sessions、close-session オペレーションを実行できます。

XML ビューにアクセスすると、ユーザは NETCONF メッセージ形式でメッセージを XML ビューにコピーして貼り付ける必要があります。NETCONF の構成中は、NETCONF の構成が失敗する可能性があるため、他の操作は行わないでください。

XML ビューで NETCONF を構成する場合、NETCONF メッセージには最後に「]] >] >] >」を追加する必要があります。追加しないと、デバイスは認識されません。

XML ビューに入ると、デバイスは自動的に自身がサポートする NETCONF 機能セットをクライアントに送信します。この場合、クライアントは自身がサポートする NETCONF 機能セットをデバイスに送信する必要があります。機能の交換が完了すると、ユーザはクライアントを使用してデバイスを構成できます。

ユーザが入力する NETCONF コマンドは、XML 言語形式の要件と『NETCONF XML API マニュアル』の構文およびセマンティック要件を満たす必要があります。NETCONF コマンドの生成を支援するサードパーティ製ソフトウェアを使用することをお勧めします。一般的には、開発およびテスト環境でコマンドラインを手動で入力します。

XML ビューを終了するには、関連する NETCONF コマンドを使用する必要があります。quit は使用できません。

XML モードでタスクを終了するためのショートカットにはキャッシュをリセットする機能があり、ショートカットの直前の内容は消去される。タスクを終了するためのショートカットキー(デフォルトは Ctrl+C)が、escape-key コマンドを使用して user-line/user-line-class view で設定されている場合、XML ビューの関連する設定に影響することがあります。例えば、 escape-key a が use-line view で配置されており、 NETCONF コマンドに文字「a」が含まれている場合、 NETCONF コマンドの最後の「a」以降しか処理できない;NETCONF コマンドに文字 「a」 が含まれていない場合、XML ビューでの設定に影響はありません。

例

#XML ビューに移動します。

<Sysname> xml

#コンピテンシーを交換します。

<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">

<capabilities>

<capability>

urn:ietf:params:netconf:base:1.0

</capability>

</capabilities>

</hello>]] >] >

#XML ビューを終了します。

<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">

<close-session/>

</rpc>]] >] >

目次

このセクションのページは **17-x-x** です。

7 章 プロセスモニタリングとメンテナンス 7-1
7.1 プロセスモニタリングとメンテナンス設定コマンド 7-1
7.1.1 display exception context 7-1
7.1.2 display exception filepath 7-3
7.1.3 display kernel deadloop 7-4
7.1.4 display kernel exception 7-7
7.1.5 display kernel reboot 7-11
7.1.6 display kernel starvation 7-14
7.1.7 exception filepath 7-17
7.1.8 process core 7-18
7.1.9 reset exception context 7-19
7.1.10 reset kernel deadloop 7-19
7.1.11 reset kernel exception 7-20
7.1.12 reset kernel reboot 7-20
7.1.13 reset kernel starvation 7-21

7章 プロセスモニタリングとメンテナンス

7.1 プロセスモニタリングとメンテナンス設定コマンド

7.1.1 display exception context

Syntax

display exception context [**count** *value*]

View

すべての view

定義済みユーザーロール

network-admin

パラメータ

count value:表示されるコンテキスト情報の数を 1 から 20 の範囲で示します。デフォルト値は 1 です。

説明

display exception context コマンドはプロセス例外に関するコンテキスト情報を表示します。

システムはプロセス例外ごとにコンテキスト情報エントリを生成する。コンテキスト情報エントリには、プロセス ID、クラッシュ時間、コアダンプファイルディレクトリ、スタック情報、およびレジスタ情報が含まれます。

例

#デバイスの例外コンテキスト情報を表示します。

<Sysname> display exception context

```
Index 1 of 1
------------------------------
Crashed slot:1
Crashed PID:2916 (macd)
Crash signal:SIGBUS
Crash time:Mon Mar 25 16:31:17 2019
Core file path:
flash:/core/node6144_macd_2916_7_-163117_1553531477.core.xz
Exception Information:
rax0 xfffffffffffffffc-4
rbx0 xffffffff4294967295
```

```
rcx0 x7f2d955c0963139833756092771
rdx0 x 11
rsi0 x7ffe19a9c660140729328977504
rdi0 x 99
rbp0 x7ffe19a9c6600 x7ffe19a9c660
rsp0 x7ffe19a9c6400 x7ffe19a9c640
r 80 x 00
r 90 x 00
r 100 xffffffff4294967295
r 110 x 293659
r 120 x6871406844736
r 130 x7ffe19a9c7f8140729328977912
Traceback (most recent call last):
File "/bin/core_translator"、 line 318, in <module>
controller.translate ()
File "/bin/core_translator"、line 274、in translate
self.update ()
File "/bin/core_translator"、line 249、in update
run_cmd (gdb_cmd)
File "/bin/core_translator"、line 77、in run_cmd
data =proc.stdout.readline ()
KeyboardInterrupt
```

表 7-1 コマンド出力

フィールド	説明
Max coredump files limited in system	デバイスに保存できるコアダンプファイルの最大数。 値がUnlimitの場合、最大数は制限されません。
Max coredump files limited for one server	サービスによって生成できるコアダンプファイルの最大数 (SCMDプロセスによって制御されない) 。 SCMDプロセスによって制御されるサービスの場合、サービスによって生成できるコアダンプファイルの最大数は、process core maxcoreコマンドの設定によって異なります。 値がUnlimitの場合、最大数は制限されません。
Total number of core dump files in system	デバイス上のコアダンプファイルの合計数。
Crashed PID	例外が発生したユーザー状態のプロセスID

フィールド	説明
Crash signal	クラッシュを引き起こした信号です。 ● SIGABRT—中断です。 ● SIGBUS—バスエラーです。 ● SIGFPE—間違った四則演算です。 ● SIGILL—不正なハードウェア指令です。 ● SIGQUIT—コントロール端末によってquit信号が送信されました。 ● SIGSEGV—不正なメモリアクセスです。 ● SIGSYS—不正なシステムコールです。 ● SIGTRAP—例外ブレークポイントのトレースです。 ● SIGXCPU—CPU使用率の制限が超過しました。 ● SIGXFSZ—ファイルサイズの制限が超過しました。 ● SIGUNKNOW—不明な理由です。
Crash time	コアファイルが作成された時間です。
Core file path	coreファイルが保存されている場所
Backtrace stopped	コアファイルが保存されているディレクトリです。

関連コマンド

- reset exception context

7.1.2 display exception filepath

Syntax

display exception filepath

View

すべての view

定義済みユーザロール

network-admin

説明

display exception filepath コマンドはコアファイルのディレクトリを表示します。

例

#core ファイルの保存パスを表示します。

<Sysname> display exception filepath

```
The exception filepath is flash:.
```

7.1.3 display kernel deadloop

Syntax

display kernel deadloop *show-number* [**offset**] [**verbose**]

View

すべての view

定義済みユーザーロール

network-admin

パラメータ

show-number: 表示するデッドループの数を指定します。設定範囲は 1～20 です。

offset: 開始デッドループと最新デッドループの間のオフセットを指定します。設定範囲は 0～19 です。デフォルトは 0 です。

verbose: 詳細情報を表示します。指定しない場合、概要情報を表示します。

説明

display kernel deadloop コマンドはカーネルスレッドのデッドループ情報を表示します。

例

#最新のカーネルスレッドのデッドループの概要を表示します。

<Sysname> display kernel deadloop 1

```
----------------- Deadloop record 1 -----------------
Description:BUG:soft lockup - CPU#0 stuck for 61![comsh:16306]
Recorded at:2019-05-0111:16:00.823018
Occurred at:2019-05-0111:16:00.823018
Instruction address:0 x4004158c
Thread:comsh (TID:16306)
Context:thread context
slot:0
Cpu:0
VCPU ID:0
Kernel module info:module name (mrpnc) module address (0 xe332a000)
```

#最近のカーネルスレッドのデッドループの詳細を表示します。

<Sysname> display kernel deadloop 1 verbose

```
----------------- Deadloop record 1 -----------------
Description:BUG:soft lockup - CPU#0 stuck for 61![comsh:16306]
Recorded at:2019-05-0111:16:00.823018
Occurred at:2019-05-0111:16:00.823018
```

```
Instruction address:0 x4004158c
Thread:comsh (TID:16306)
Context:thread context
slot:0
Cpu:0
VCPU ID:0
Kernel module info:module name (mrpnc) module address (0 xe332a000)

Last 5 thread ACes :migration/0 (11:16:00.823018)-->
swapper (11:16:00.833018)-->
kthreadd (11:16:00.833518)-->
swapper (11:16:00.833550)-->
disk (11:16:00.833560)

Register content:
Reg:r 0、Val=0 x00000000 ;Reg:r 1、Val=0 xe2be5ea0 ;
Reg:r 2、Val=0 x00000000 ;Reg:r 3、Val=0 x77777777 ;
Reg:r 4、Val=0 x00000000 ;Reg:r 5、Val=0 x00001492 ;
Reg:r 6、Val=0 x00000000 ;Reg:r 7、Val=0 x0000ffff ;
Reg:r 8、Val=0 x77777777 ;Reg:r 9、Val=0 x00000000 ;
Reg:r 10、Val=0 x00000001 ;Reg:r 11、Val=0 x0000002c ;
Reg:r 12、Val=0 x057d9484 ;Reg:r 13、Val=0 x00000000 ;
Reg:r 14、Val=0 x00000000 ;Reg:r 15、Val=0 x02000000 ;
Reg:r 16、Val=0 xe2be5f00 ;Reg:r 17、Val=0 x00000000 ;
Reg:r 18、Val=0 x00000000 ;Reg:r 19、Val=0 x00000000 ;
Reg:r 20、Val=0 x024c10f8 ;Reg:r 21、Val=0 x057d9244 ;
Reg:r 22、Val=0 x00002000 ;Reg:r 23、Val=0 x0000002c ;
Reg:r 24、Val=0 x00000002 ;Reg:r 25、Val=0 x24000024 ;
Reg:r 26、Val=0 x00000000 ;Reg:r 27、Val=0 x057d9484 ;
Reg:r 28、Val=0 x0000002c ;Reg:r 29、Val=0 x00000000 ;
Reg:r 30、Val=0 x0000002c ;Reg:r 31、Val=0 x00000000 ;
Reg:cr, Val=0 x84000028 ;Reg:nip、Val=0 x057d9550 ;
Reg:xer、Val=0 x00000000 ;Reg:lr, Val=0 x0186eff0 ;
Reg:ctr, Val=0 x682f7344 ;Reg:msr、Val=0 x00784b5c ;
Reg:trap, Val=0 x0000b030 ;Reg:dar, Val=0 x77777777 ;
Reg:dsisr、Val=0 x40000000 ;Reg:result、Val=0 x00020300 ;

Dump stack (total 1024 bytes、16 bytes/line):
0 xe2be5ea0:02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0 xe2be5eb0:00 00 00 04 00 00 00 00 00 00 28 05 8 d 34 c4
0 xe2be5ec0:02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0 xe2be5ed0:02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5ee0:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
0 xe2be5ef0:95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f00:a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f10:00 00 00 00 00 00 00 00 01 e9 00 00
0 xe2be5f20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f30:00 00 00 00 00 02 be 66 c0 02 be 66 d0
0 xe2be5f40:02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0 xe2be5f50:02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0 xe2be5f60:02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0 xe2be5f70:05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0 xe2be5f80:02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0 xe2be5f90:00 03 00 00 00 00 02 be 5f e0 00 00 00 30
0 xe2be5fa0:02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0 xe2be5fb0:02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0 xe2be5fc0:02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0 xe2be5fd0:02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0 xe2be5fe0:00 00 00 00 00 00 00 00 02 be 60 18
0 xe2be5ff0:02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0 xe2be6000:02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0 xe2be6010:02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0 xe2be6020:02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0 xe2be6030:02 27 00 00 00 00 00 00 00 02 be 60 68
0 xe2be6040:02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0 xe2be6050:00 00 00 04 02 21 00 00 00 00 00 01 e9 00 00
0 xe2be6060:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be6070:00 00 00 00 00 02 be 66 c0 02 be 66 d0
0 xe2be6080:02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0 xe2be6090:00 00 00 02 21 00 00 05 8 d 34 c4 05 7d 92 44

Call trace:
Function Address =0 x8012a4b4
Function Address =0 x8017989c
Function Address =0 x80179b30
Function Address =0 x80127438
Function Address =0 x8012d734
Function Address =0 x80100a00
Function Address =0 xe0071004
Function Address =0 x8016ce0c
Function Address =0 x801223a0

Instruction dump:
41 a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4 bfffe6c 80780290 7f64db78 4804ea35 <807 f002c> 3880 万 38 a00080 3863000c
```

表 7-2 コマンド出力

フィールド	説明
Description	CPU番号、スレッド実行時間、スレッド名、スレッド番号など、カーネルスレッドデッドループの説明です。
Recorded at	カーネルスレッドデッドループが記録された時間(マイクロ秒単位の精度)です。
Occurred at	カーネルスレッドのデッドループが発生した時刻(マイクロ秒精度)です。
Instruction address	カーネルスレッドデッドループの命令アドレスです。
Thread	カーネルスレッドデッドループの名前と番号です。
Context	カーネルスレッドデッドループのコンテキストです。
Cpu	カーネルスレッドが実行されたCPUの番号です。
VCPU ID	カーネルスレッドが実行されたCPUの番号です。
Kernel module info	カーネルスレッドがデッドループを検出したときに、システムにロードされていたカーネルモジュールの情報。 ● module nameはカーネルモジュール名です。 ● module addressカーネルモジュールがロードするメモリアドレス
Last 5 thread ACes	カーネルスレッドがデッドループを検出した場合、デッドループが発生したCPU上の、直近5回のカーネルスレッド切替え履歴を記録する。カーネルスレッドの名前と、マイクロ秒単位のカーネルスレッド切り替えポイントが含まれます。
Register content	カーネルスレッドがデッドループを検出したときのレジスタ情報。Regはレジスタ名、 Valはレジスタに格納されている値を表します。
Dump stack	カーネルスレッドがデッドループを検出したときのスタック情報
Call trace	カーネルスレッドがデッドループを検出したときの関数呼び出しスタック情報です。
Instruction dump	カーネルスレッドがデッドループを検出したときに対応する命令コード。不正なコマンドはffffffffで表されます。
No information to display	システムにカーネルスレッドのデッドループレコードはありません。

関連コマンド

- reset kernel deadloop

7.1.4 display kernel exception

Syntax

display kernel exception *show-number* [*offset*] [**verbose**]

View

すべての view

定義済みユーザーロール

network-admin

パラメータ

show-number: 表示するカーネル例外の数を指定します。設定範囲は 1～20 です。

offset: 開始例外と最新例外の間のオフセットを指定します。設定範囲は 0～19 です。デフォルトは 0 です。

verbose: 詳細情報を表示します。指定しない場合、コマンドは概要情報を表示します。

説明

display kernel exception コマンドは、カーネルスレッドの例外情報を表示します。

実行中のカーネルスレッドに例外が発生すると、システムは自動的に例外情報を記録します。

例

#最新のカーネルスレッド例外の概要を表示します。

<Sysname> display kernel exception 1

```
----------------- Exception record 1 -----------------
Description:Oops [#0]
Recorded at:2019-05-0111:16:00.823018
Occurred at:2019-05-0111:16:00.823018
Instruction address:0 x4004158c
Thread:comsh (TID:16306)
Context:thread context
slot:0
Cpu:0
VCPU ID:0
Kernel module info:module name (mrpnc) module address (0 xe332a000)
module name (disk) module address (0 xe00bd000)
```

#最新のカーネルスレッド例外の詳細を表示します。

<Sysname> display kernel exception 1 verbose

```
----------------- Exception record 1 -----------------
Description:Oops [#0]
Recorded at:2019-05-0111:16:00.823018
Occurred at:2019-05-0111:16:00.823018
Instruction address:0 x4004158c
Thread:comsh (TID:16306)
Context:thread context
```

```
slot:0
Cpu:0
VCPU ID:0
Kernel module info:module name (mrpnc) module address (0 xe332a000)
module name (12500) module address (0 xe00bd000)

Last 5 thread ACes :migration/0 (11:16:00.823018)-->
swapper (11:16:00.833018)-->
kthreadd (11:16:00.833518)-->
swapper (11:16:00.833550)-->
disk (11:16:00.833560)

Register content:
Reg:r 0、Val=0 x00000000 ;Reg:r 1、Val=0 xe2be5ea0 ;
Reg:r 2、Val=0 x00000000 ;Reg:r 3、Val=0 x77777777 ;
Reg:r 4、Val=0 x00000000 ;Reg:r 5、Val=0 x00001492 ;
Reg:r 6、Val=0 x00000000 ;Reg:r 7、Val=0 x0000ffff ;
Reg:r 8、Val=0 x77777777 ;Reg:r 9、Val=0 x00000000 ;
Reg:r 10、Val=0 x00000001 ;Reg:r 11、Val=0 x0000002c ;
Reg:r 12、Val=0 x057d9484 ;Reg:r 13、Val=0 x00000000 ;
Reg:r 14、Val=0 x00000000 ;Reg:r 15、Val=0 x02000000 ;
Reg:r 16、Val=0 xe2be5f00 ;Reg:r 17、Val=0 x00000000 ;
Reg:r 18、Val=0 x00000000 ;Reg:r 19、Val=0 x00000000 ;
Reg:r 20、Val=0 x024c10f8 ;Reg:r 21、Val=0 x057d9244 ;
Reg:r 22、Val=0 x00002000 ;Reg:r 23、Val=0 x0000002c ;
Reg:r 24、Val=0 x00000002 ;Reg:r 25、Val=0 x24000024 ;
Reg:r 26、Val=0 x00000000 ;Reg:r 27、Val=0 x057d9484 ;
Reg:r 28、Val=0 x0000002c ;Reg:r 29、Val=0 x00000000 ;
Reg:r 30、Val=0 x0000002c ;Reg:r 31、Val=0 x00000000 ;
Reg:cr, Val=0 x84000028 ;Reg:nip、Val=0 x057d9550 ;
Reg:xer、Val=0 x00000000 ;Reg:lr, Val=0 x0186eff0 ;
Reg:ctr, Val=0 x682f7344 ;Reg:msr、Val=0 x00784b5c ;
Reg:trap, Val=0 x0000b030 ;Reg:dar, Val=0 x77777777 ;
Reg:dsisr、Val=0 x40000000 ;Reg:result、Val=0 x00020300 ;

Dump stack (total 1024 bytes、16 bytes/line):
0 xe2be5ea0:02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0 xe2be5eb0:00 00 00 04 00 00 00 00 00 00 28 05 8 d 34 c4
0 xe2be5ec0:02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0 xe2be5ed0:02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5ee0:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5ef0:95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f00:a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
```

```
0 xe2be5f10:00 00 00 00 00 00 00 01 e9 00 00
0 xe2be5f20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f30:00 00 00 00 00 02 be 66 c0 02 be 66 d0
0 xe2be5f40:02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0 xe2be5f50:02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0 xe2be5f60:02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0 xe2be5f70:05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0 xe2be5f80:02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0 xe2be5f90:00 03 00 00 00 00 02 be 5f e0 00 00 00 30
0 xe2be5fa0:02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0 xe2be5fb0:02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0 xe2be5fc0:02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0 xe2be5fd0:02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0 xe2be5fe0:00 00 00 00 00 00 00 00 02 be 60 18
0 xe2be5ff0:02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0 xe2be6000:02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0 xe2be6010:02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0 xe2be6020:02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0 xe2be6030:02 27 00 00 00 00 00 00 00 02 be 60 68
0 xe2be6040:02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0 xe2be6050:00 00 00 04 02 21 00 00 00 00 00 01 e9 00 00
0 xe2be6060:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be6070:00 00 00 00 00 02 be 66 c0 02 be 66 d0
0 xe2be6080:02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0 xe2be6090:00 00 00 02 21 00 00 05 8 d 34 c4 05 7d 92 44

Call trace:
Function Address =0 x8012a4b4
Function Address =0 x8017989c
Function Address =0 x80179b30
Function Address =0 x80127438
Function Address =0 x8012d734
Function Address =0 x80100a00
Function Address =0 xe0071004
Function Address =0 x8016ce0c
Function Address =0 x801223a0

Instruction dump:
41 a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4 bfffe6c 80780290 7f64db78 4804ea35 <807 f002c> 3880 万 38 a00080 3863000c
```

このコマンドの表示情報の詳細については、表 7-3 を参照してください。

関連コマンド

- reset kernel exception

7.1.5 display kernel reboot

Syntax

display kernel reboot *show-number* [*offset*] [**verbose**]

View

すべての view

定義済みユーザーロール

network-admin

パラメータ

show-number: 表示するリブートの数を指定します。設定範囲は 1～20 です。

offset: 開始リブートと最新のリブートの間のオフセットを指定します。設定範囲は 0～19 です。デフォルトは 0 です。

verbose: 詳細情報を表示します。指定しない場合、コマンドは概要情報を表示します。

説明

display kernel reboot コマンドは、デバイスの再起動情報を表示します。

例

#最新の再起動サマリー情報を表示します。

<Sysname> display kernel reboot 1

```
---------------- Reboot record 1 -----------------
Recorded at:2019-05-0111:16:00.823018
Occurred at:2019-05-0111:16:00.823018
Reason:0 x 31
Thread:comsh (TID:16306)
Context:thread context
slot:0
Target Slot:0
Cpu:0
VCPU ID:0
Kernel module info:module name (mrpnc) module address (0 xe332a000)
module name (12500) module address (0 xe00bd000)
```

#最新の再起動の詳細を表示します。

<Sysname> display kernel reboot 1 verbose

```
---------------- Reboot record 1 -----------------
```

```
Recorded at:2019-05-0111:16:00.823018
Occurred at:2019-05-0111:16:00.823018
Reason:0 x 31
Thread:comsh (TID:16306)
Context:thread context
slot:0
Target Slot:0
Cpu:0
VCPU ID:0
Kernel module info:module name (mrpnc) module address (0 xe332a000)
module name (12500) module address (0 xe00bd000)

Last 5 thread ACes :migration/0 (11:16:00.823018)-->
swapper (11:16:00.833018)-->
kthreadd (11:16:00.833518)-->
swapper (11:16:00.833550)-->
disk (11:16:00.833560)

Dump stack (total 1024 bytes、16 bytes/line):
0 xe2be5ea0:02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0 xe2be5eb0:00 00 00 04 00 00 00 00 00 00 28 05 8 d 34 c4
0 xe2be5ec0:02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0 xe2be5ed0:02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5ee0:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5ef0:95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f00:a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f10:00 00 00 00 00 00 00 00 01 e9 00 00
0 xe2be5f20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f30:00 00 00 00 00 02 be 66 c0 02 be 66 d0
0 xe2be5f40:02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0 xe2be5f50:02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0 xe2be5f60:02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0 xe2be5f70:05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0 xe2be5f80:02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0 xe2be5f90:00 03 00 00 00 00 02 be 5f e0 00 00 00 30
0 xe2be5fa0:02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0 xe2be5fb0:02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0 xe2be5fc0:02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0 xe2be5fd0:02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0 xe2be5fe0:00 00 00 00 00 00 00 00 02 be 60 18
0 xe2be5ff0:02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0 xe2be6000:02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0 xe2be6010:02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
```

```
0 xe2be6020:02 be 60 40 00 00 00 00 00 00 00 02 be 60 98
0 xe2be6030:02 27 00 00 00 00 00 00 00 02 be 60 68
0 xe2be6040:02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0 xe2be6050:00 00 00 04 02 21 00 00 00 00 00 01 e9 00 00
0 xe2be6060:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be6070:00 00 00 00 00 02 be 66 c0 02 be 66 d0
0 xe2be6080:02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0 xe2be6090:00 00 00 02 21 00 00 05 8 d 34 c4 05 7d 92 44

Call trace:
Function Address =0 x8012a4b4
Function Address =0 x8017989c
Function Address =0 x80179b30
Function Address =0 x80127438
Function Address =0 x8012d734
Function Address =0 x80100a00
Function Address =0 xe0071004
Function Address =0 x8016ce0c
Function Address =0 x801223a0
```

表 7-3 コマンド出力

フィールド	説明
Recorded at	再起動が記録された時刻です。単位はマイクロ秒です。
Occurred at	リブートが発生した時刻です。単位はマイクロ秒です。
Reason	再起動の理由
Thread	再起動時に実行されるカーネルスレッドの名前と番号
Context	再起動が発生したコンテキストです。
slot	再起動をトリガしたスロットの番号です。
Target Slot	再起動したスロットの番号です。
Cpu	再起動をトリガしたCPUの番号です。
VCPU ID	リブートをトリガしたCPUコアの数です。
Kernel module info	再起動時にロードされたカーネルモジュールに関する情報(カーネルモジュール名やメモリアドレスなど)です。
Last 5 thread ACes	リブート前にCPUで発生した最後の5つのカーネルスレッドスイッチ(カーネルスレッド名とカーネルスレッドの切り替え時点を含む、マイクロ秒単位の精度)です。
Dump stack	再起動が発生したときに実行されていたスレッドのスタック情報です。
Call trace	関数呼び出しスタック情報です。
No information to display	再起動情報が存在しません。

関連コマンド

- reset kernel reboot

7.1.6 display kernel starvation

Syntax

display kernel starvation show-number [*offset*] [**verbose**]

View

すべての view

定義済みユーザーロール

network-admin

パラメータ

show-number：表示するスターベーション情報の数 (1 ～ 20)。

offset：最も近いエントリから表示される開始エントリのオフセット。値の範囲は 0 ～ 19 です。デフォルト値は 0 です。

verbose：詳細情報が表示されることを示します。このパラメータが指定されていない場合、サマリー情報が表示されます。

説明

display kernel starvation コマンドを使用して、カーネルスレッドの空き情報を表示します。

例

#最近のカーネルスレッドのスターベーションの概要を表示します。

<Sysname> display kernel starvation 1

```
----------------- Starvation record 1 -----------------
Description:information:task comsh:16306 blocked for more than 10 seconds.
Recorded at:2019-05-0111:16:00.823018
Occurred at:2019-05-0111:16:00.823018
Instruction address:0 x4004158c
Thread:comsh (TID:16306)
Context:thread context
slot:0
Cpu:0
VCPU ID:0
Kernel module info:module name (mrpnc) module address (0 xe332a000)
module name (12500) module address (0 xe00bd000)
```

#最近のカーネルスレッドのスターベーションの詳細を表示します。

<Sysname> display kernel starvation 1 verbose

```
----------------- Starvation record 1 -----------------
Description:information:task comsh:16306 blocked for more than 10 seconds.
Recorded at:2019-05-0111:16:00.823018
Occurred at:2019-05-0111:16:00.823018
Instruction address:0 x4004158c
Thread:comsh (TID:16306)
Context:thread context
slot:0
Cpu:0
VCPU ID:0
Kernel module info:module name (mrpnc) module address (0 xe332a000)
module name (12500) module address (0 xe00bd000)

Last 5 thread ACes :migration/0 (11:16:00.823018)-->
swapper (11:16:00.833018)-->
kthreadd (11:16:00.833518)-->
swapper (11:16:00.833550)-->
disk (11:16:00.833560)

Register content:
Reg:r 0、Val=0 x00000000 ;Reg:r 1、Val=0 xe2be5ea0 ;
Reg:r 2、Val=0 x00000000 ;Reg:r 3、Val=0 x77777777 ;
Reg:r 4、Val=0 x00000000 ;Reg:r 5、Val=0 x00001492 ;
Reg:r 6、Val=0 x00000000 ;Reg:r 7、Val=0 x0000ffff ;
Reg:r 8、Val=0 x77777777 ;Reg:r 9、Val=0 x00000000 ;
Reg:r 10、Val=0 x00000001 ;Reg:r 11、Val=0 x0000002c ;
Reg:r 12、Val=0 x057d9484 ;Reg:r 13、Val=0 x00000000 ;
Reg:r 14、Val=0 x00000000 ;Reg:r 15、Val=0 x02000000 ;
Reg:r 16、Val=0 xe2be5f00 ;Reg:r 17、Val=0 x00000000 ;
Reg:r 18、Val=0 x00000000 ;Reg:r 19、Val=0 x00000000 ;
Reg:r 20、Val=0 x024c10f8 ;Reg:r 21、Val=0 x057d9244 ;
Reg:r 22、Val=0 x00002000 ;Reg:r 23、Val=0 x0000002c ;
Reg:r 24、Val=0 x00000002 ;Reg:r 25、Val=0 x24000024 ;
Reg:r 26、Val=0 x00000000 ;Reg:r 27、Val=0 x057d9484 ;
Reg:r 28、Val=0 x0000002c ;Reg:r 29、Val=0 x00000000 ;
Reg:r 30、Val=0 x0000002c ;Reg:r 31、Val=0 x00000000 ;
Reg:cr, Val=0 x84000028 ;Reg:nip、Val=0 x057d9550 ;
Reg:xer、Val=0 x00000000 ;Reg:lr, Val=0 x0186eff0 ;
Reg:ctr, Val=0 x682f7344 ;Reg:msr、Val=0 x00784b5c ;
Reg:trap, Val=0 x0000b030 ;Reg:dar, Val=0 x77777777 ;
Reg:dsisr、Val=0 x40000000 ;Reg:result、Val=0 x00020300 ;
```

```
Dump stack (total 1024 bytes、16 bytes/line):
0 xe2be5ea0:02 be 5e c0 24 00 00 24 00 00 00 00 05 7d 94 84
0 xe2be5eb0:00 00 00 04 00 00 00 00 00 00 28 05 8 d 34 c4
0 xe2be5ec0:02 be 60 a0 01 86 ef f0 00 00 00 00 00 00 00 00
0 xe2be5ed0:02 04 05 b4 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5ee0:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5ef0:95 47 73 35 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f00:a0 e1 64 21 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f10:00 00 00 00 00 00 00 00 01 e9 00 00
0 xe2be5f20:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be5f30:00 00 00 00 00 02 be 66 c0 02 be 66 d0
0 xe2be5f40:02 be 61 e0 00 00 00 02 00 00 00 00 02 44 b3 a4
0 xe2be5f50:02 be 5f 90 00 00 00 08 02 be 5f e0 00 00 00 08
0 xe2be5f60:02 be 5f 80 00 ac 1b 14 00 00 00 00 00 00 00 00
0 xe2be5f70:05 b4 5f 90 02 be 5f e0 00 00 00 30 02 be 5f e0
0 xe2be5f80:02 be 5f c0 00 ac 1b f4 00 00 00 00 02 45 00 00
0 xe2be5f90:00 03 00 00 00 00 02 be 5f e0 00 00 00 30
0 xe2be5fa0:02 be 5f c0 00 ac 1b 14 61 f1 2e ae 02 45 00 00
0 xe2be5fb0:02 44 b3 74 02 be 5f d0 00 00 00 30 02 be 5f e0
0 xe2be5fc0:02 be 60 60 01 74 ff f8 00 00 00 00 00 00 08 00
0 xe2be5fd0:02 be 5f f0 00 e8 93 7e 02 be 5f f8 02 be 5f fc
0 xe2be5fe0:00 00 00 00 00 00 00 00 02 be 60 18
0 xe2be5ff0:02 be 60 10 00 e9 65 98 00 00 00 58 00 00 2a 4f
0 xe2be6000:02 be 60 10 00 00 00 00 00 00 00 00 02 be 60 68
0 xe2be6010:02 be 60 40 00 e8 c6 a0 00 00 11 17 00 00 00 00
0 xe2be6020:02 be 60 40 00 00 00 00 00 00 00 00 02 be 60 98
0 xe2be6030:02 27 00 00 00 00 00 00 00 02 be 60 68
0 xe2be6040:02 be 60 60 00 00 00 01 00 00 b0 30 02 be 60 98
0 xe2be6050:00 00 00 04 02 21 00 00 00 00 00 01 e9 00 00
0 xe2be6060:00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0 xe2be6070:00 00 00 00 00 02 be 66 c0 02 be 66 d0
0 xe2be6080:02 be 61 e0 00 00 00 02 00 00 00 00 02 be 61 70
0 xe2be6090:00 00 00 02 21 00 00 05 8 d 34 c4 05 7d 92 44

Call trace:
Function Address =0 x8012a4b4
Function Address =0 x8017989c
Function Address =0 x80179b30
Function Address =0 x80127438
Function Address =0 x8012d734
Function Address =0 x80100a00
Function Address =0 xe0071004
Function Address =0 x8016ce0c
```

```
Function Address =0 x801223a0

Instruction dump:
41 a2fe9c 812300ec 800200ec 7f890000 409efe8c 80010014 540b07b9 40a2fe80
4 bfffe6c 80780290 7f64db78 4804ea35 <807 f002c> 38800000 38 a00080 3863000c
```

このコマンドの表示情報の詳細については、表 7-3 を参照してください。

関連コマンド

- reset kernel starvation

7.1.7 exception filepath

Syntax

exception filepath *directory*

undo exception filepath *directory*

デフォルト

コアファイルのファイルは flash:/に保存されます。

View

User view

定義済みユーザーロール

network-admin

パラメータ

directory : コアファイルを保存するディレクトリを指定します。

説明

exception filepath コマンドは、コアファイルの保存するディレクトリを設定します。

undo exception filepath コマンドは、指定されたディレクトリを削除します。

コアファイルを保存するディレクトリは、デフォルトのファイルシステムのルートディレクトリです。

例

コアファイルを保存するディレクトリを flash:/に指定します。

<AC> exception filepath flash:/

関連コマンド

- display exception filepath
- process core

7.1.8 process core

Syntax

process core { **maxcore** *value* | **off** } { **job** *job-id* | **name** *process-name* }

デフォルト

同じユーザープロセスは、最初の例外が発生したときにコアファイルを生成し、その後の例外に対してはコアファイルを生成しません。

View

User view

定義済みユーザーロール

network-admin

パラメータ

off: コアファイルの作成を無効にします。

maxcore *value*: コアファイルの作成を有効にし、コアファイルの最大数を設定します。設定範囲は 1～10 です。

name *process-name*: プロセス名を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別しません。

job *job-id*: job ID でプロセスを指定します。設定範囲は 1～2147483647 です。プロセスを再起動しても、job ID は変わりません。

説明

process core コマンドは例外のコアファイルを作成するプロセスを有効あるいは無効にし、コアファイルの最大数を設定します。

process core コマンドはプロセスのすべてのインスタンスに適用します。

コマンドは、コアファイルが最大数になるまで、指定されたプロセスがクラッシュするたびに、コアファイルを作成することを有効にします。コアファイルは例外情報を記録します。

コアファイルがシステム記憶リソースを消費するため、例外情報のレビューする必要がないプロセスはコアファイルの生成を無効にすることができます。

例

プロセス routed のコアファイルの作成を無効にします。

<AC> process core off name routed

プロセス routed のコアファイルの作成を有効にし、コアファイルの最大数を 5 に設定します。

<AC> process core maxcore 5 name routed

関連コマンド

- display exception context
- exception filepath

7.1.9 reset exception context

Syntax

reset exception context

View

User view

定義済みユーザーロール

network-admin

説明

reset exception context コマンドはプロセス例外のコンテキスト情報を削除します。

例

プロセス例外のコンテキスト情報を削除します。

<AC> reset exception context

関連コマンド

- display exception context

7.1.10 reset kernel deadloop

Syntax

reset kernel deadloop

View

User view

定義済みユーザーロール

network-admin

説明

reset kernel deadloop コマンドはカーネルスレッドのデッドループ情報を削除します。

例

カーネルスレッドのデッドループ情報を削除します。

<AC> reset kernel deadloop

関連コマンド

- display kernel deadloop

7.1.11 reset kernel exception

Syntax

reset kernel exception

View

User view

定義済みユーザーロール

network-admin

説明

reset kernel exception コマンドはカーネルスレッドの例外情報を削除します。

例

カーネルスレッドの例外情報を削除します。

<AC> reset kernel exception

関連コマンド

- display kernel exception

7.1.12 reset kernel reboot

Syntax

reset kernel reboot

View

User view

定義済みユーザーロール

network-admin

説明

reset kernel reboot コマンドはカーネルスレッドの再起動情報を削除します。

例

カーネルスレッドの再起動情報を削除します。

<AC> reset kernel reboot

関連コマンド

- display kernel reboot

7.1.13 reset kernel starvation

Syntax

reset kernel starvation

View

User view

定義済みユーザーロール

network-admin

説明

reset kernel starvation コマンドを使用して、カーネルスレッドの空き情報を削除します。

例

#カーネルスレッドの空き情報を削除します。

<Sysname> reset kernel starvation

関連コマンド

- display kernel starvation

目次

このセクションのページは **17-x-x** です。

8 章 ポートミラーリング 8-1
8.1 ポートミラーリング設定コマンド 8-1
8.1.1 display mirroring-group 8-1
8.1.2 mirroring-group 8-2
8.1.3 mirroring-group mirroring-port (interface view) 8-3
8.1.4 mirroring-group mirroring-port (system view) 8-4
8.1.5 mirroring-group monitor-port (interface view) 8-5
8.1.6 mirroring-group monitor-port (system view) 8-6

8章 ポートミラーリング

8.1 ポートミラーリング設定コマンド

8.1.1 display mirroring-group

Syntax

display mirroring-group { *group-id* | **all** | **local** }

View

すべての view

定義済みユーザーロール

network-admin

network-operator

パラメータ

group-id: ミラーリンググループの番号を 1～2 の範囲で指定します。

all: すべてのミラーリンググループを指定します。

local: ローカルミラーリンググループを指定します。

説明

display mirroring-group コマンドを使用して、ミラーリンググループを表示します。

ミラーリンググループの情報には、ミラーリンググループのタイプ、ステータス、内容が含まれます。ミラーリンググループ番号でソートされます。

例

すべてのミラーリンググループに関する情報を表示します。

<Sysname> display mirroring-group all

```
Mirroring group 1:
Type:Local
Status:Active
Mirroring port:GigabitEthernet1/0/1 Inbound
Monitor port:GigabitEthernet1/0/2
```

表 8-1 コマンド出力

フィールド	説明する
Mirroring group	ミラーグループの番号

フィールド	説明する
Type	ミラーグループのタイプ: ● Local:ローカルミラーグループ
Status	ミラーグループの状態: ● Active:ミラーグループが有効であることを示します。 ● Incomplete:ミラーグループの割り当てが完了していないため、まだ有効ではありません
Mirroring port	送信元ポート
Monitor port	宛先ポート

8.1.2 mirroring-group

Syntax

mirroring-group *group-id* local

undo mirroring-group { *group-id* | **all** | **local** }

デフォルト

ミラーリンググループは存在しません

View

System-view

定義済みユーザーロール

network-admin

パラメータ

group-id: ミラーリンググループの番号を 1～2 の範囲で指定します。

local: ローカルミラーリンググループを指定します。

all: すべてのミラーリンググループを指定します。

説明

mirroring-group コマンドを使用して、ミラーリンググループを作成します。

undo mirroring-group コマンドを使用して、ミラーリンググループを削除します。

例

ローカルミラーリンググループを作成します。

<AC> system-view

[AC] mirroring-group 1 local

8.1.3 mirroring-group mirroring-port (interface view)

Syntax

mirroring-group *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id* **mirroring-port**

デフォルト

ポートは、ミラーリンググループの送信元ポートとして機能しません。

View

Interface view

定義済みユーザーロール

network-admin

パラメータ

group-id: 1～2 の範囲内の番号でミラーリンググループを指定します。指定したミラーリンググループが既に存在している必要があります。

both: 受信パケットと送信パケットの両方をミラーリングします。

inbound: 受信パケットのみミラーリングします。

outbound: 送信パケットのみミラーリングします。

説明

mirroring-group mirroring-port コマンドを使用して、ポートをミラーリンググループの送信元ポートとして設定します。

undo mirroring-group mirroring-port コマンドを使用して、デフォルトを復元します。

ポートは、1 つのミラーリンググループの送信元ポートとして機能できます。

送信元ポートはモニタポートとして使用できません。

例

ローカルミラーリンググループ 1 を作成して、GigabitEthernet 1/0/1 の双方向トラフィックを監視します。

<AC> system-view

[AC] mirroring-group 1 local

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] mirroring-group 1 mirroring-port both

関連コマンド

- mirroring-group

8.1.4 mirroring-group mirroring-port (system view)

Syntax

mirroring-group *group-id* **mirroring-port** *interface-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *group-id mirroring-port* **interface-list**

デフォルト

ミラーリンググループに送信元ポートが設定されていません。

View

System-view

定義済みユーザーロール

network-admin

パラメータ

group-id: 1～2 の範囲内の番号でミラーリンググループを指定します。指定したミラーリンググループが既に存在している必要があります。

interface-list: 8 つまでのポート項目のスペース区切りのリストを指定します。各項目は、単一のポートまたはポート範囲を *interface-type interface-number1* ～*interface-type interface-number2* の形式で指定します。指定されたインタフェースは同じタイプで、同じカードでなければなりません。*interface-number2* 引数の値は、*interface-number1* 引数の値以上でなければなりません。

both: 受信パケットと送信パケットの両方をミラーリングします。

inbound: 受信パケットのみミラーリングします。

outbound: 送信パケットのみミラーリングします。

説明

mirroring-group mirroring-port コマンドを使用して、ミラーリンググループの送信元ポートを設定します。

undo mirroring-group mirroring-port コマンドを使用して、ミラーリンググループからソースポートを削除します。

ポートは、1 つのミラーリンググループの送信元ポートとして機能できます。

送信元ポートはモニタポートとして使用できません。

例

ローカルミラーリンググループ 1 を作成して、GigabitEthernet 1/0/1 の双方向トラフィックを監視します。

<AC> system-view

[AC] mirroring-group 1 local

[AC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both

関連コマンド

- mirroring-group

8.1.5 mirroring-group monitor-port (interface view)

Syntax

mirroring-group *group-id* **monitor-port**

undo mirroring-group *group-id* **monitor-port**

デフォルト

ポートは、ミラーリンググループのモニタポートとして機能しません

View

Interface view

定義済みユーザーロール

network-admin

パラメータ

group-id: 1～2 の範囲内の番号でミラーリンググループを指定します。

説明

mirroring-group monitor-port コマンドを使用して、ミラーリンググループのモニタポートとして設定します。

undo mirroring-group monitor-port コマンドはデフォルトに戻します。

ミラーリンググループのモニタポートでスパニングツリー機能を有効にしないでください。

ポートミラーリングにのみモニタポートを使用するため、データ監視デバイスはミラーリングされたトラフィックのみを受信して分析します。

既存のミラーリンググループのポートをモニタポートとして設定しないでください。

例

ローカルミラーリンググループ 1 を作成し、モニタポートとして GigabitEthernet 1/0/1 を設定します。

<AC> system-view

[AC] mirroring-group 1 local

[AC] interface gigabitethernet 1/0/1

[AC-GigabitEthernet1/0/1] mirroring-group 1 monitor-port

関連コマンド

- mirroring-group

8.1.6 mirroring-group monitor-port (system view)

Syntax

mirroring-group *group-id* **monitor-port** *interface-list*

undo mirroring-group *group-id* **monitor-port** *interface-list*

デフォルト

設定なし

View

System-view

定義済みユーザーロール

network-admin

パラメータ

group-id: 1～2 の範囲内の番号でミラーリンググループを指定します。

interface-type interface-number:宛先ポートを示します。ここで、*interface-type interface-number* はポートタイプとポート番号です。

説明

mirroring-group monitor-port コマンドを使用して、ミラーリンググループのモニタポートを設定します。

undo mirroring-group monitor-port コマンドを使用して、ミラーリンググループからモニタポートを削除します。

ミラーリンググループのモニタポートでスパニングツリー機能を有効にしないでください。

ポートミラーリングにのみモニタポートを使用するため、データ監視デバイスはミラーリングされたトラフィックのみを受信します。

既存のミラーリンググループのポートをモニタポートとして設定しないでください。

例

ローカルミラーリンググループ 1 を作成し、モニタポートとして GigabitEthernet 1/0/1 を設定します。

<AC> system-view

[AC] mirroring-group 1 local

[AC] mirroring-group 1 monitor-port gigabitethernet 1/0/1

関連コマンド

- mirroring-group

目次

このセクションのページは **17-x-x** です。

9 章 パケットキャプチャ 9-1
9.1 パケットキャプチャ設定コマンド 9-1
9.1.1 display packet-capture status 9-1
9.1.2 packet-capture local ap 9-2
9.1.3 packet-capture stop 9-4

9章 パケットキャプチャ

9.1 パケットキャプチャ設定コマンド

9.1.1 display packet-capture status

Syntax

display packet-capture status

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display packet-capture status コマンドを使用して、パケットキャプチャステータス情報を表示します。

例

AP1 の無線 1 のパケットキャプチャステータス情報を表示します。

<AC> display packet-capture status

```
Status     : Capturing
File Name  : flash:/a.pcap
User Name  : N/A
Password   : N/A
```

表 9-1 コマンド出力

フィールド	説明
Status	パケットキャプチャステータスです。現在のソフトウェアバージョンでは**Capturing**テータスのみがサポートされています。
File name	キャプチャデータが保存されたファイル名です。
Username	リモートFTPサーバにログインするためのユーザ名です。

フィールド	説明
Password	リモートFTPサーバにログインするためのパスワードです。暗号文と平文のそれぞれのパスワードは******として表示されます。パスワードが必要でないか設定されていない場合、このフィールドには**N/A**が表示されます。

関連コマンド

- **packet-capture local ap**

9.1.2 packet-capture local ap

Syntax

packet-capture local ap *ap-name* **radio** *radio-id* [**capture-filter** *capt-expression* | **limit-frame-size** *bytes* | **autostop filesize** *kilobytes* | **autostop duration** *seconds*] * **write url** *url* [**username** *username* [**password** { **cipher** | **simple** } *key*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

ap-name : AP 名を指定します。AP 名は、文字、数字、アンダースコア（_）、ドット（.）、左括弧（[）、右括弧（]）、スラッシュ（/）、ハイフン（-）を含む 1～64 文字の文字列です。大文字と小文字を区別します。

radio *radio-id* : ID でラジオを指定します。

capture-filter *capt-expression* ： キャプチャするパケットに一致する条件式を指定します。1～64 文字の文字列です。大文字と小文字を区別します。キャプチャフィルタ条件式を指定しない場合、装置はインタフェース上のすべての受信パケットをキャプチャします。

limit-frame-size *bytes* ： パケットをキャプチャする最大バイト数を設定します。値の範囲は 64～8000 バイトで、デフォルト値は 8000 バイトです。パケットのフレーム長がフレームサイズ制限を超えていても 9196 バイト以下の場合、システムは最初のバイトから開始して、パケットから指定されたバイト数だけをキャプチャします。フレーム長が 9196 バイトを超える場合、システムはパケットをキャプチャしません。

autostop filesize *kilobytes* ： ファイルローテーションが無効になっているときに最大パケットファイルサイズを超えた場合、パケットのキャプチャを停止します。*kilobytes* 引

数は、ファイルの最大サイズを設定します。値の範囲は 1～65536 キロバイトです。制限を設定しない場合、ファイルのサイズは無制限です。

autostop duration *seconds*：キャプチャ時間が終了したときにパケットのキャプチャを停止します。*seconds* 引数はキャプチャ時間を設定します。値の範囲は 1～2147483647 秒です。制限を設定しない場合、キャプチャ時間は無制限です。

write url *url*：キャプチャされたパケットデータを格納する FTP サーバ上のファイルの URL を指定します。URL は 1～255 文字の大文字小文字を区別する文字列である必要があります。URL 文字列には、アットマーク（@）、および指定されたユーザ名とパスワードを使用できません。URL を指定しないと、キャプチャされたパケットデータは保存されません。

username *username* : FTP サーバにログインするためのユーザ名を指定します。ユーザ名は、大文字と小文字を区別する 1～32 文字です。

password : FTP サーバにログインするためのパスワードを指定します。

cipher：暗号文のパスワードを指定します。

simple：平文のパスワードを指定します。

key：パスワードを指定します。この引数は大文字と小文字を区別します。**simple** を指定する場合は、1～32 文字の文字列でなければなりません。**cipher** を指定する場合は、1～73 文字の暗号文字列でなければなりません。

説明

packet-capture local ap コマンドを使用して、AP 無線で受信したパケットをキャプチャし、キャプチャしたパケットを FTP サーバ上のファイルに保存します。

パケットのキャプチャ中にキャプチャを停止するには、**packet-capture stop** コマンドを使用します。

autostop filesize オプションと **autostop duration** オプションのそれぞれを設定した場合、停止オプションの制限のいずれかに達すると、パケットキャプチャが停止します。

URL、ユーザ名、パスワードを指定するには、次の制限事項とガイドラインに従ってください。

- FTP サーバの IP アドレスが IPv4 アドレスの場合は、*ftp://FTP server address:port number/file* の形式で URL を入力します。
- サーバアドレスフィールドの DNS ドメイン名を指定することもできます。URL の形式は *ftp://DNS domain name/file name* です。
- ユーザ名とパスワードは、FTP サーバで設定されているものと同じである必要があります。サーバがユーザ名のみを認証する場合、パスワードは省略できます。

autostop duration *seconds* オプションで短いキャプチャ時間を設定しないでください。時間が短すぎると、FTP サーバにログインしていないときにキャプチャが停止することがあります。その場合キャプチャされたパケットは、パケットファイルが作成されていないため保存できません。

例

AP1 の無線 1 で受信パケットをキャプチャします。

<AC> packet-capture local ap ap1 radio 1 write url ftp://10.1.1.1/database.pcap username 1 password simple 1

関連コマンド

- **display packet-capture status**
- **packet-capture stop**

9.1.3 packet-capture stop

Syntax

packet-capture stop

View

ユーザ view

定義済みユーザロール

network-admin

説明

packet-capture stop コマンドを使用して、パケットキャプチャを停止します。

階層型ネットワーク上のローカル AC がオフラインになると、センターAC は、ローカル AC に接続された AP のパケットキャプチャ管理プロセスを停止します。ただし、AP でのパケットキャプチャは継続されます。パケットキャプチャを停止するには、AP のセンターAC 上でパケットキャプチャを再度有効にして、このコマンドを実行する必要があります。

例

パケットキャプチャを停止します。

<AC> packet-capture stop

関連コマンド

- **packet-capture local ap**

目次

このセクションのページは **17-x-x** です。

10 章 NetMeister 10-1
10.1 Netmeister コマンド 10-1
10.1.1 display netmeister 10-1
10.1.2 netmeister account 10-3
10.1.3 netmeister alarm enable notice 10-5
10.1.4 netmeister enable 10-5
10.1.5 netmeister event log enable 10-6
10.1.6 netmeister event syslog enable 10-7
10.1.7 netmeister management ip 10-8
10.1.8 netmeister mode parent 10-9
10.1.9 netmeister parent 10-10
10.1.10 netmeister parent-mode mqtt port 10-11
10.1.11 netmeister parent-mode sitename 10-12
10.1.12 netmeister proxy 10-13
10.1.13 netmeister update 10-14
10.1.14 netmeister track 10-15

10章 NetMeister

10.1 Netmeisterコマンド

10.1.1 display netmeister

Syntax

display netmeister

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display netmeister コマンドは NetMeister 及び親機との接続情報を表示します。

例

子機モードの装置で NetMeisetr 及び親機との接続情報を表示します。

<Switch> display netmeister

```
NetMeister state                              : Enabled
Mode                                           : Child
Connection state with NetMeister              : Connected
Account name                                  : nec
Proxy information:
  State                                  : Connected
  URL                                   : http://www.abc.com:8080
  Username                              : admin
Parent 1:
  IP address                                  : 192.168.0.254
  Port number                                 : 443
  Connection state                            : Connected
Parent 2:
  IP address                                  : 192.168.0.255
  Port number                                 : 8443
  Connection state                            : Connected
```

親機モードの装置で NetMeisetr との接続情報を表示します。

<Switch> display netmeister

```
NetMeister state                          : Enabled
Mode                                       : Parent
Connection state with NetMeister          : Connected
Account name                               : nec
Proxy information:
State                                     :  --
Parent information:
Site name                                 : test
Interval                                  : 3600 sec
MQTT interval                             : 60 sec
MQTT status                               : Connected
```

表 10-1 コマンド出力

フィールド	説明
NetMeister state	NetMeister機能の状態です。 ● **Enabled** —有効 ● **Disabled** —無効
Mode	NetMeisterへの接続モードです。 ● **Parent** —親機モード ● **Child** —子機モード
Connection state with NetMeister	NetMeisterとの接続状況です。 ● **Connected.**—接続 ● **Disconnected.**—切断
Account name	グループIDです。
Proxy information	NetMeisterプロキシサーバとの接続に関する情報です。
State	プロキシサーバへの接続状態です。 ● **Connected.**—接続 ● **Disconnected.**—切断 ● **"--"** —プロキシサーバを設定していない場合に表示されます。
URL	プロキシサーバのURL。形式はhttp :// <domain>:<ポート>です。domainはプロキシサーバのWebアドレスまたはIPアドレス、portはポート番号です。 プロキシサーバが構成されていない場合、このフィールドは表示されません。
IP address	親機のIPアドレスです。 子機モード時のみ表示されます。

フィールド	説明
Port number	親機のポート番号です。 子機モード時のみ表示されます。
Connection state	NetMeister機能による親機への接続状態です。 • **Connected.**—接続 • **Disconnected.**—切断 子機モード時のみ表示されます。
Site name	拠点名です。 親機モード時のみ表示されます。
Interval	親機の更新情報の送信間隔です。 親機モード時のみ表示されます。
MQTT interval	MQTTプロトコルの送信間隔です。 親機モード時のみ表示されます。
MQTT status	MQTTプロトコルの接続状態です。 • **Connected.**—接続 • **Disconnected.**—切断 • **"--"** —接続が成功しなかった場合に表示されます。 親機モード時のみ表示されます。

関連コマンド

- **netmeister account**
- **netmeister enable**
- **netmeister parent**

10.1.2 netmeister account

Syntax

netmeister account *account* **password** { **cipher** | **simple** } *string*

undo netmeister account

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

account: グループ ID を 2～31 文字の文字列で設定します。文字列に使用できるのは小文字、数字、およびハイフン(-)のみで、ハイフン(-)で開始または終了することはできません。

cipher: 暗号テキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

string: プレーンテキスト形式のパスワードは 8～31 文字の文字列で設定します。暗号化形式のパスワードは 41～73 文字の文字列で設定します。

説明

netmeister account コマンドを使用して、親機への子機認証と NetMeister への装置登録で使用するグループ ID とパスワードを設定します。

undo netmeister account コマンドは、設定したグループ ID とパスワードを削除します。

このコマンドを複数回実行すると、最新の設定が有効になります。実行するたびに、デバイスが NetMeister プラットフォームから切断され、新しく指定したユーザ名とパスワードで再接続されます。

設定の失敗を避けるために、ユーザ名とパスワードを指定する前に、デバイスで NetMeister が無効になっていることを確認してください。

指定したユーザ名とパスワードが、親機および NetMeister プラットフォームで設定されているユーザ名とパスワードと同じであることを確認してください。

例

親機への子機認証と NetMeister への装置登録のために、グループ ID **nec** と プレーンテキストのパスワード **nec1234** を装置に設定します。

<Switch> system-view

[Switch] netmeister account nec password simple nec1234

関連コマンド

- **display netmeister**
- **netmeister enable**

10.1.3 netmeister alarm enable notice

🕮 **メモ:**

netmeister alarm enable notice コマンドは Version 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister alarm enable notice

undo netmeister alarm enable notice

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister alarm enable notice コマンドによって NetMeister の注意レベルのアラーム生成を有効にします。

undo netmeister alarm enable notice コマンドによって NetMeister の注意レベルの NetMeister アラーム生成を無効にします。

この機能により、システムは次のイベントの注意レベルのアラームを生成できます。

- Telnet、ssh などを使用してログインまたはログアウトした場合
- 設定を保存した場合
- 設定を保存しないまま 5 分が経過した場合

例

NetMeister の注意レベルのアラームの生成を有効にします。

<Switch> system-view

[Switch] netmeister alarm enable notice

10.1.4 netmeister enable

Syntax

netmeister enable

undo netmeister enable

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister enable コマンドによって NetMeister 機能を有効にします。

undo netmeister enable コマンドによってデフォルトに戻します。

子デバイス、親機、および NetMeister プラットフォームが設定されていることを確認します。この機能により、デバイスは NetMeister ネットワークで子デバイスとして動作できます。

例

NetMeister 機能を有効にします。

<Switch> system-view

[Switch] netmeister enable

関連コマンド

- **display netmeister**

10.1.5 netmeister event log enable

Syntax

netmeister event log enable

undo netmeister event log enable

デフォルト

有効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister event log enable コマンドは NetMeister 機能が有効な時、端末がアソシエーションフェーズまたは認証フェーズで接続に失敗した際のイベントログを 5 分間隔で NetMeister に通知します。

undo netmeister event log enable コマンドはイベントログの送信を停止します。

例

イベントログの送信を停止する。

<Switch> system-view

[Switch] undo netmeister event log enable

関連コマンド

- **netmeister enable**

10.1.6 netmeister event syslog enable

🕮 **メモ:**

netmeister event syslog enable コマンドは Version 9.6.08c を含む以降のソフトウェアからサポートしています。本コマンドはバージョンアップで自動的に有効になります。

Syntax

netmeister event syslog enable

undo netmeister event syslog enable

View

System-view

デフォルト

有効

定義済みユーザロール

network-admin

説明

netmeister event syslog enable コマンドは NetMeister 機能が有効な時、logbuffer に出力されたログを 5 分間隔で NetMeister にイベントログとして通知します。

undo netmeister event syslog enable コマンドは logbuffer に出力されるログを NetMeister にイベントログとして通知する動作を停止します。

netmeister event syslog enable コマンドは **netmeister enable** が有効な状態でも変更できます。

🕮 **メモ:**

netmeister event syslog enable コマンドは logbuffer に出力されたログを通知するため、**info-center source** *module-name* **logbuffer deny** コマンドによって logbuffer への出力をモジュール単位で無効にした場合はイベントログにも通知されなくなります。Information Center の詳細は QX-W2300AC シリーズアクセスコントローラオペレーションマニュアルの“3 *システム管理*” の“*Information Center*”を参照してください。

10.1.7 netmeister management ip

Syntax

netmeister management ip *ip-address*

undo netmeister management ip

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister management ip コマンドによって NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを設定します。

undo netmeister management ip コマンドによってデフォルトに戻します。

NetMeister 機能については NetMeister が提供している操作ガイドを参照してください。

例

NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを 10.1.1.10 に設定します。

```
<Sysname> system-view
[Sysname] netmeister management ip 10.1.1.10
```

10.1.8 netmeister mode parent

Syntax

netmeister mode parent

undo netmeister mode parent

デフォルト

子機モード

View

System-view

定義済みユーザロール

network-admin

説明

netmeister mode parent コマンドを利用して NetMeister への接続モード親機モードにします。親機モードは NetMeister 機能を有する親機ルータがいない環境において、NetMeisterPrime(有償サービス)を利用して NetMeister で管理する場合に利用します。NetMeister 機能を有する親機ルータがある環境では、それらの機器を親機とし、子機モードで利用して下さい。

undo netmeister mode parent コマンドを利用して NetMeister への接続モードを子機モードに戻します。

netmeister mode parent コマンドを設定する前に、**netmeister enable** や子機モード時に利用する **netmeister parent** コマンドが無効になっていることを確認してください。

NetMeister ネットワークには、次のロールが含まれている必要があります。

- **Child**:管理対象のデバイス。
- **Parent**:すべての子デバイスを NetMeister に接続するデバイス。親機は子デバイスを認証し、認証された子デバイスに NetMeister メッセージを発行します。
- **NetMeister**:ネットワーク管理者が親機から子デバイスを管理および維持するためのクラウドプラットフォーム。

例

NetMeister 機能を有する親機ルータがいない環境で QX を NetMeister によって管理するために、親機モードを設定します。

<Switch> system-view

[Switch] netmeister mode parent

関連コマンド

- **netmeister enable**
- **display netmeister**

10.1.9 netmeister parent

Syntax

netmeister parent ip *ip-address* [**port** *port-number*]

undo netmeister parent ip *ip-address*

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 親機の IP アドレスを設定します。

port *port-number*: 親機のポート番号を 1～65535 の範囲で設定します。デフォルトのポート番号は 443 です。

説明

netmeister parent ip コマンドは、子機モードとして NetMeister に接続する際に、親機とする機器の IP アドレスとポート番号を設定します。

undo netmeister parent ip を使用して、子機として接続する親機の IP アドレスとポート番号を削除します。

netmeister parent ip コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister parent コマンドと **netmeister account** コマンドを設定し、**netmeister enable** コマンドを有効にすると、子機は認証応答を受信するまで親機に子機認証の要求を送信します。**netmeister parent** コマンドが複数設定されている場合、装置は設定されたすべてのアドレスに要求を送信し、それぞれの親機との接続を確立します。これにより、親機の障害によるサービスの中断を防ぎ、ネットワークの可用性が向上します。最大で 2 つまで親機 IP アドレスを設定できます。

例

IP アドレス **192.168.0.254** ポート番号 443 の親機に接続する子機として設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.0.254 port 443

IP アドレス **192.168.1.254** の親機に接続する子機として設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.1.254

関連コマンド

- **display netmeister**
- **netmeister enable**

10.1.10 netmeister parent-mode mqtt port

Syntax

netmeister parent-mode mqtt port *port-number*

undo netmeister mode parent

デフォルト

8883

View

System-view

定義済みユーザロール

network-admin

パラメータ

port-number: MQTT プロトコルのポート番号を 443 もしくは 8883 で設定します。

説明

netmeister parent-mode mqtt port コマンドを利用して親機モードの QX が NetMeister に接続する際の MQTT プロトコルのポート番号を変更します。

undo netmeister mode parent コマンドを利用して NetMeister に接続する際の MQTT プロトコルのポート番号をデフォルトに戻します。

親機と NetMeister は、Message Queuing Telemetry Transport (MQTT) を TCP で相互通信します。

この設定を行うと、親機と NetMeister の間のセッションが終了します。次に、デバイスは新しく指定されたポートを使用して、NetMeister プラットフォームへの接続を再確立します。

このコマンドは、NetMeister が有効の場合にのみ有効です。

例

NetMeister に接続するためにネットワーク環境で 8883 を開放する必要がない様に、MQTT のポート番号を 443 に変更します。

<Switch> system-view

[Switch] netmeister parent-mode mqtt port 443

関連コマンド

- **display netmeister**
- **netmeister enable**

10.1.11 netmeister parent-mode sitename

Syntax

netmeister parent-mode sitename *name*

undo netmeister parent-mode sitename

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

name: 親機のサイト名を 2 から 31 文字の文字列で指定します。小文字、数字、およびハイフン(-)のみが使用でき、文字列をハイフンで開始または終了することはできません。

説明

netmeister parent-mode sitename コマンドを利用して親機モードの QX が NetMeister に接続する際の拠点名を設定します。

undo netmeister mode parent コマンドを利用して拠点名の設定を削除します。

親機の場合は、NetMeister を有効にする前に親サイト名を指定する必要があります。

例

親機モードで NetMeister に接続するために拠点名 test を設定します。

<Switch> system-view

[Switch] netmeister parent-mode sitename test

関連コマンド

- **display netmeister**
- **netmeister enable**

10.1.12 netmeister proxy

Syntax

netmeister proxy url *url* [**username** *username* **password** { **cipher | simple** } *string*]

undo netmeister proxy

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

url *url*:プロキシサーバの URL を指定します。***http://***<*domain*>*:*<*port*>形式で、大文字と小文字を区別して 8 から 128 文字の文字列を指定します。<*domain*>引数はプロキシサーバのドメイン名または IP アドレスを表し、<*port*>引数は 1 から 65535 の範囲のポート番号を表します。デフォルトのポート番号は 80 です。HTTP 経由で URL にアクセスできることを確認します。

username *username*:プロキシサーバへのアクセスに使用するユーザ名を指定します。1 から 31 文字の大文字と小文字が区別されます。文字列には、バックスラッシュ、引用符 (") 、疑問符 (?) 、スペースを含めることはできません。

password:プロキシサーバへのアクセスに使用するパスワードを指定します。

cipher:パスワードを暗号化形式で指定します。

simple:プレーンテキスト形式でパスワードを指定します。セキュリティ上の理由から、プレーンテキスト形式で指定されたパスワードは暗号化形式で保存されます。

string:パスワード文字列を指定します。プレーンテキスト形式は、大文字と小文字を区別する 1 から 31 文字の文字列です。暗号化された形式は、大文字と小文字を区別した 33 から 73 文字の文字列です。プレーンテキストのパスワードには、バックスラッシュ、引用符 (") 、疑問符 (?) 、またはスペースを含めることはできません。

説明

netmeister proxy コマンドは装置が NetMeister 宛の https 通信のために指定された proxy サーバを利用します。親機への https 通信にはプロキシサーバを使用しません。

undo netmeister proxy コマンドはプロキシサーバの指定を削除します。

このコマンドを実行する前に、NetMeister が無効になっていることを確認してください。

ユーザ名とパスワードを指定しない場合、子デバイスはユーザ名またはパスワードを持たずにプロキシサーバにアクセスしようとします。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

IP アドレス **192.168.1.254** の親機に接続する子機とし、NetMeister にはプロキシサーバ 10.1.1.254 (ポート:8080)を使用するように設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.1.254

[Switch] netmeister proxy url http://10.1.1.254:8080

関連コマンド

- **netmeister enable**
- **display netmeister**

10.1.13 netmeister update

🕮 **メモ:**

netmeister update コマンドは Version 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister update

View

すべての view

定義済みユーザロール

network-admin

説明

netmeister update コマンドは NetMeister に登録している装置情報を即時更新します。

例

装置名を変更した後、NetMeister に登録している装置情報を即時更新します。

<AP> system-view

[AP] sysname test

[AP] netmeister update

無線子機の装置名を ap10 から ap9 に変更した後、NetMeister に登録している装置情報を即時更新します。

<AP> system-view

[AP] wlan rename-ap ap10 ap9

[AP] netmeister update

10.1.14 netmeister track

🕮 **メモ:**

netmeister track コマンドは Version 9.4.09 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister track *track-entry-number*

undo netmeister track *track-entry-number*

View

System-view

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

track *track-entry-number*: 1～1024 の範囲の番号で指定されたトラックエントリに NetMeister 機能を紐付けます。

説明

netmeister track コマンドは、トラックエントリを NetMeister 機能に関連付けます。

undo netmeister track コマンドは、NetMeister 機能 とトラック エントリの関連付けを解除します。

本コマンドは NetMeister から Ping 監視設定をした場合に自動で設定されます。NetMeister から Ping 監視設定を削除した場合に自動で設定が解除されます。

本コマンドが適用されるトラックエントリは以下の条件と一致する NQA エントリのみです。NetMeister から Ping 監視設定をした場合、本条件と一致する設定が行われます。

- **nqa entry** コマンドで設定された *admin-name* は **nm-ping** である必要があります。

- **type** コマンドで設定された NQA テストタイプは **icmp-echo** である必要があります。
- **reaction checked-element probe-fail** コマンドでリアクションエントリが設定されている必要があります。