GVT-222833-001-00 1.13

QX-W610 アクセスポイント

コマンドマニュアル

改版履歴

版数	日付	改版内容
1.00	2023/09	初版発行
1.01	2023/10	・「セクション 7 WLAN セキュリティ」の「2 章 WIPS」を将来サポートに修正しました。
1.02	2024/03	・誤記訂正 ・「セクション 6 AP 管理」の「LED 点灯モードの設定」に **customer** モードを追加しました。 ・「セクション 7 WLAN セキュリティ」の「2 章 WIPS」をサポートに変更しました。 ・「セクション 8 Radio リソース管理」の OFDMA、BSS カラーリング、TWT ネゴシエーションのデフォルト値に説明を追加しました。 ・「セクション 8 Radio リソース管理」の **channel** コマンドの説明を更新しました。 ・「セクション 11 WLAN 拡張機能」に「WLAN の高可用性の設定」を追加しました。 ・「セクション 14 QoS」に下記コマンドを追加しました。 ・**atf** ・「セクション 15 ネットワーク管理とモニタ」の「6 章 Netmeister」に下記コマンドを追加しました。 ・**netmeister alarm enable notice** ・**netmeister management ip** ・**netmeister update** ・**netmeister track** ・「セクション 16 高可用性」を追加しました。
1.03	2024/09	・「セクション 8 Radio リソース管理」の「1 章 無線管理」に下記コマンドを追加しました。 ・**short-gi** ・**protection-mode**

版数	日付	改版内容
1.04	2024/09	・「セクション 01 基本設定」の「5 章 ファイルシステム管理」の下記コマンドの説明を追加しました。 ・**dir** ・「セクション 02 システム管理」の「1 章 装置管理」の下記コマンドの注意書きを追加しました。 ・**memory-threshold** ・「セクション 05 WLAN アクセス」の下記のコマンドを削除しました。 ・**client-mode** コマンド ・**display client-mode** コマンド ・「セクション 07 WLAN セキュリティ」の下記のコマンドの説明を更新しました。 ・**pmf association-comeback** ・「セクション 08 Radio リソース管理」の下記のコマンドの説明を追加しました ・**max-power**
1.05	2024/10	・「セクション 07 WLAN セキュリティ」に下記のコマンドの説明を追加しました。 ・**akm sae pwe** ・「セクション 14 QoS」の「2 章 WLAN QoS」の下記コマンドの説明を更新しました。 ・**qos trust**
1.06	2024/12	・「セクション 5-WLAN」の「1 章 WLAN アクセス」の下記コマンドの説明を修正しました。 ・**display wlan client** ・「セクション 3-インタフェース」の「2 章 Ethernet インタフェース」の下記コマンドの説明を修正しました。 ・**jumboframe enable**

版数	日付	改版内容
1.07	2025/01	・「セクション 2 システム管理」の「1 章 装置管理」の下記のコマンドの説明を更新しました。 ・「1.1.7 diag boot-info display」の説明を更新しました。 ・「1.1.20 display version」の説明を更新しました。 ・「セクション 5 WLAN アクセス」の「1 章 WLAN アクセス」の下記のコマンドの説明を更新しました。 ・「1.1.14 display wlan client」の説明を更新しました。 ・「1.1.43 wlan client idle-timeout」のデフォルト値を変更しました。 ・「セクション 6 AP 管理」の「1 章 AP 管理」の下記のコマンドを追加しました。 ・「1.1.1 radar-channel-switchback」コマンドを追加しました。 ・「セクション 7 WLAN セキュリティ」の「1 章 WLAN セキュリティ」の下記のコマンドの説明を更新しました。 ・「1.1.21 wpa3」のコマンドについて、説明を更新しました。 ・「セクション 8 Radio リソース管理」の「1 章 Radio の管理と設定」の下記のコマンドの説明を追加しました。 ・「1.1.34 shutdown (Radio interface view)」コマンドの説明を追加しました。 ・「セクション 15 ネットワーク管理とモニタ」の「3 章 SNMP」に下記コマンドを追加しました。 ・「3.1.11 simulate snmp-trap」コマンドを追加しました。
1.08	2025/01	・「セクション 02 システム管理」の「1 章 装置管理」の下記コマンドのデフォルト設定の説明を更新しました。 ・「1.1.6 copyright-info enable」のコマンドについて、説明を更新しました。 ・「1.1.27 password-recovery enable」のコマンドについて、説明を更新しました。
1.09	2025/03	・「セクション 12 ユーザアクセスと認証」の以下の説明を更新しました ・「3.2.8 local-user」
1.10	2025/03	・「セクション 04 ネットワーク」の説明を更新しました。 ・「セクション 08 WLAN セキュリティ」の説明を更新しました。 ・「セクション 12 ユーザアクセスと認証」の説明を更新しました。

版数	日付	改版内容
1.11	2026/03	・「セクション 02 システム管理」の「1 章 装置管理」の下記コマンドを追加しました。 **・restore factory-default** ・「セクション 04 ネットワーク」の「5 章 LLDP」下記コマンドの説明を更新しました。 **・display lldp local-information** ・「セクション 11 WLAN 拡張機能」の「1 章 WLAN 最適化」の下記コマンドを追加しました。 **・option keep-active** ・「セクション 15 ネットワーク管理」の「6 章 Netmister」の下記コマンドの説明を更新しました。 **・netmeister alarm enable notice**
1.12	2026/07	・「セクション 06 Radio リソース管理」の「1 章 Radio の管理と設定」の下記コマンドの Syntax を更新しました。 **・a-msdu** ・「セクション 06 Radio リソース管理」の「1 章 Radio の管理と設定」に、下記コマンドを追加しました。 **・wlan global-configuration** ・「セクション 08-WLAN セキュリティ」の「2 章 WIPS」に、無線通信と WIPS センサの併用に関する説明を追加しました。 ・「セクション 09-WLAN ローミング」の「1 章 WLAN ローミング」に、下記コマンドの説明を修正しました。 **・ft enable** ・「セクション 09-WLAN ローミング」の「1 章 WLAN ローミング」に、WLAN 802.11v 関連の下記コマンドを追加しました。 **・bss transition-management disassociation** **・bss transition-management enable** **・sacp anti-sticky** ・誤記訂正

版数	日付	改版内容
1.13	2026/11	・「セクション 01-基本機能」の「1 章 CLI」に、下記コマンドを追加しました。 ・**repeat** ・「セクション 04-ネットワーク接続」の「4 章 スパニングツリー」の下記コマンドのデフォルト値の誤記を修正しました。 ・**stp pathcost-standard** ・「セクション 08-WLAN セキュリティ」の「1 章 WLAN セキュリティ」の下記コマンドの **private-psk** パラメータは未サポートであるため削除しました。 ・**akm mode**

Copyright © NEC Corporation 2023 - 2026

All Rights Reserved

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

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- 本装置は *QX-W610 アクセスポイント コマンドマニュアル*に記載されているコマンドのみ使用することができます。*QX-W610 アクセスポイントコマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

バージョン

本マニュアルに対応する製品バージョンは Version 7.5.98 を含む以降のソフトウェアです。

関連マニュアル

次のマニュアルには、QX-W610 アクセスポイントに関する詳細な説明があります

マニュアル	内容
QX-W610 アクセスポイント インスタレーションマニュアル	システムのインストールについて説明しています。
QX-W610 アクセスポイント オペレーションマニュアル	機能の設定について説明しています。
QX-W610 アクセスポイント コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-W610 アクセスポイント Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。

マニュアルの構成

このコマンドマニュアルは以下のセクションで構成されます。

- **基本機能**

  アクセス方法、ファイルシステム管理、ソフトウェア管理の設定について説明します。

- **システム管理**

  装置管理、NTP、Information Center の設定について説明します。

- **インタフェース**

  Ethernet ポートの設定について説明します。

- **ネットワーク**

  MAC アドレス、VLAN、IP アドレス、DHCP 等の設定について説明します。

- **WLAN アクセス**

  WLAN アクセスの設定について説明します。

- **AP 管理**

  AP 管理の設定について説明します

- **WLAN セキュリティ**

  WLAN セキュリティ WIPS の設定について説明します。

- **Radio リソース管理**

  無線管理、無線リソースの管理、バンドナビゲーション等の設定について説明します。

- **WLAN ローミング**

  WLAN ローミングの設定について説明します。

- **WLAN トラフィック**

  ユーザアイソレーションの設定について説明します。

- **WLAN 拡張機能**

  WLAN 最適化の設定について説明します。

- **ユーザアクセスと認証**

  AAA、RADIUS、802.1X、MAC アドレス認証等の設定について説明します

- **セキュリティ**

  ACL、タイムレンジ、SSH 等の設定について説明します。

- **QoS**

  QoS、WLAN QoS の設定について説明します。

- **ネットワーク管理とモニタ**

  SNMP、モニタリングとメンテナンス、NetMeister 等の設定について説明します。

- **高可用性**

  Track の設定について説明します。

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンド表記規則

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

II. GUI 表記規則

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

III. キーボード操作

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

IV. マウス操作

表記規則	説明
クリック	マウスのボタンを素早く押します。特に指定がない場合は左ボタンを押します。
ダブルクリック	マウスの左ボタンを素早く 2 回押します。
ドラッグ	マウスの左ボタンを押したまま移動します。

V. 記号

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

VI. ネットワークアイコン

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

VII. 設定例

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

VIII. セキュリティ強化

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

本マニュアルは以下に示す 16 個のセクションで構成されています。

01-基本機能

02-システム管理

03-インタフェース

04-ネットワーク

05-AP 管理

06-Radio リソース管理

07-WLAN アクセス

08-WLAN セキュリティ

09-WLAN ローミング

10-WLAN トラフィック

11-WLAN 拡張機能

12-ユーザアクセスと認証

13-セキュリティ

14-QoS

15-ネットワーク管理とモニタ

16-高可用性

QX-W610 アクセスポイント

コマンドマニュアル

01. 基本機能

本マニュアルは以下に示す章で構成されています。

01-CLI
02-ロールベースアクセスコントロール(RBAC)
03-ログイン
04-FTP と TFTP
05-ファイルシステム管理
06-コンフィグレーションファイル管理
07-ソフトウェアアップグレード

目次

このセクションのページは **1-x-x** です。

1 章 CLI 1-1
1.1 基本 CLI コマンド 1-1
1.1.1 alias 1-1
1.1.2 display | { count | { begin | exclude | include } } 1-3
1.1.3 display | by-linenum 1-5
1.1.4 display > 1-7
1.1.5 display >> 1-8
1.1.6 display alias 1-10
1.1.7 display history-command 1-11
1.1.8 display history-command all 1-12
1.1.9 display hotkey 1-14
1.1.10 hotkey 1-16
1.1.11 quit 1-18
1.1.12 repeat 1-18
1.1.13 return 1-20
1.1.14 screen-length disable 1-20
1.1.15 system-view 1-22

1章 CLI

1.1 基本CLIコマンド

1.1.1 alias

Syntax

alias *alias command*

undo alias *alias*

デフォルト

表 1-1 にシステム定義のエイリアスを示します。

表 1-1 システム定義のコマンドエイリアス

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

View

System view

定義済みユーザロール

network-admin

パラメータ

alias: エイリアスを指定します。設定範囲は 1～20 文字です。大文字、小文字を区別します。エイリアスは **alias** あるいはスペースを使用することができません。

command: コマンドの文字列を指定します。コマンドの文字列は Syntax の要件に一致している必要があります。

説明

alias コマンドはコマンドのエイリアスを設定します。

undo alias コマンドはコマンドのエイリアスを削除します。

システムで定義したエイリアスは削除することができません。

コマンドあるいはコマンドのパラメータで開始するエイリアスを設定することができます。設定後はコマンドを実行するためにエイリアスを使用することができます。**undo** で始まるコマンドがある場合についても、エイリアスを使用することができます。

たとえば、**display ip routing-table** コマンドのエイリアス **siprt** を設定すると、**display ip routing-table** コマンドを実行するために、**siprt** コマンドを入力することが可能です。

display ip コマンドのエイリアスに **ship** コマンドを設定した場合、**display ip** で始まるすべてのコマンドを実行するため、**ship** を使用することができます。

- **display ip routing-table** コマンドを実行するため **ship routing-table** コマンドを入力します。
- **display ip interface** コマンドを実行するため **ship interface** コマンドを入力します。

コマンド文字列は最大 9 つのパラメータまで含むことができます。各パラメータはドル記号（$）と 1～9 までのシーケンス番号で開始します。たとえば、**display ip $1 | include $2** を行うためにエイリアス **shinc** を設定できます。**display ip interface | include GigabitEthernet1/0/1** コマンドを実行する場合、**shinc interface GigabitEthernet1/0/1** を入力することで実行することができます。

例

 # display ip routing-table コマンドを行うためにエイリアス **shiprt** を設定し、設定を確認します。

<AP> system-view

[AP] alias shiprt display ip routing-table

[AP] shiprt

```
Destinations : 14 Routes : 14
Destination/Mask      Proto   Pre Cost      NextHop         Interface
0.0.0.0/0             Static  60  0         192.168.100.1   Vlan1
0.0.0.0/32            Direct  0   0         127.0.0.1       InLoop0
127.0.0.0/8           Direct  0   0         127.0.0.1       InLoop0
127.0.0.1/32          Direct  0   0         127.0.0.1       InLoop0
127.255.255.255/32    Direct  0   0         127.0.0.1       InLoop0
192.168.0.0/24        Direct  0   0         192.168.0.167   Vlan1
192.168.0.167/32      Direct  0   0         127.0.0.1       InLoop0
192.168.0.255/32      Direct  0   0         192.168.0.167   Vlan1
192.168.100.0/24      Direct  0   0         192.168.100.167 Vlan1
192.168.100.167/32    Direct  0   0         127.0.0.1       InLoop0
192.168.100.255/32    Direct  0   0         192.168.100.167 Vlan1
224.0.0.0/4           Direct  0   0         0.0.0.0         NULL0
224.0.0.0/24          Direct  0   0         0.0.0.0         NULL0
255.255.255.255/32    Direct  0   0         127.0.0.1       InLoop0
```

 # display $1 | include $2 コマンドを行うためにエイリアス **shinc** を設定し、すべてのスタティックルート情報を表示するためにエイリアス **shinc** を使用します。

<AP> system-view

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

[AP] shinc routing-table Static

```
0.0.0.0/0         Static  60  0         192.168.100.1   Vlan1
```

関連コマンド

display alias

1.1.2 display | { count | { begin | exclude | include } }

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

count: コマンド出力の指定した行数を表示します。

begin: 指定した正規表現の文字列を含む行を含む以降の行を表示します。

exclude: 指定した正規表現の文字列を含まない行を表示します。

include: 指定した正規表現の文字列を含む行を表示します。

regular-expression: 1～256 字の大文字と小文字を区別した正規表現を指定します。

説明

display | { **begin** | **exclude** | **include** }コマンドは正規表現を使用して **display** コマンドから出力をフィルタします。

正規表現の詳細は、オペレーションマニュアルのセクション 1 *基本機能 "CLI の概要"*を参照してください。

例

カレントコンフィグレーションで vlan を含む行を表示します。

<AP> display current-configuration | include **vlan**

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

1.1.3 display | by-linenum

Syntax

display *command* **| by-linenum**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

説明

display | by-linenum コマンドは **display** コマンドに行番号をつけて表示します。

行番号を使用することで、わかりやすく表示することができます。

行番号は 5 桁で表示され、コロン（:）あるいはハイフン（-）が続きます。**display | by-linenum** コマンドと **display | begin regular-expression** コマンドを同時に使用した場合、正規表現に一致しないすべての行はハイフン（-）で表示されます。

例

VLAN999 の設定を表示するため、行番号をつけて出力を表示します。

<AP> display vlan 999 | by-linenum

```
  1:  VLAN ID: 999
  2:  VLAN type: Static
  3:  Route interface: Configured
  4:  IPv4 address: 192.168.2.1
  5:  IPv4 subnet mask: 255.255.255.0
  6:  Description: For LAN Access
  7:  Name: VLAN 0999
  8:  Tagged ports:  None
  9:  Untagged ports:
 10:    GigabitEthernet1/0/1
```

カレントコンフィグレーションで **user-group** で始まる行から以降の行を表示します。

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

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

```
116-  return
```

1.1.4 display >

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

filename: 出力を保存するファイル名を 1～63 文字で指定します。

説明

display >コマンドは **display** コマンドの出力を別のファイルに保存します。

display コマンドは設定、統計情報、装置の状態を表示します。**display >**コマンドはファイルに **display** コマンドの出力を保存します。

指定したファイルが存在しない場合、ファイルを新規に作成し、ファイルに **display** コマンドの出力を保存します。指定したファイルが存在する場合、ファイルに上書きします。

例

vlan.txt というファイルに VLAN 1 の設定を保存します。

<AP> display vlan 1 > vlan.txt

vlan.txt ファイルの内容を確認します。

<AP> more vlan.txt

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

1.1.5 display >>

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

command: **display** コマンドのキーワードと引数を指定します。有効なキーワードと引数を表示する場合、**display ?**と入力します。

filename: 出力を保存するファイル名を 1～63 文字で指定します。

説明

display >>コマンドは **display** コマンドの出力をファイルの最後に追記します。

display コマンドは設定、統計情報、装置の状態を表示します。**display >>**コマンドはファイルに **display** コマンドの出力を保存します。

指定したファイルが存在しない場合、ファイルを新規に作成し、ファイルに **display** コマンドの出力を保存します。指定したファイルが存在する場合、ファイルの最後に追記します。

例

vlan.txt というファイルの最後に VLAN 999 を追記します。

<AP> display vlan 999 >> vlan.txt

<AP>

vlan.txt ファイルの内容を確認します。

<AP> more vlan.txt

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

```
VLAN ID: 999
VLAN type: Static
Route interface: Configured
IPv4 address: 192.168.2.1
IPv4 subnet mask: 255.255.255.0
Description: For LAN Access
Name: VLAN 0999
Tagged ports:   None
Untagged ports:
  GigabitEthernet1/0/1
```

1.1.6 display alias

Syntax

display alias [*alias*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

alias: コマンドエイリアスを指定します。指定しない場合、すべてのコマンドのエイリアスを表示します。

説明

display alias コマンドはコマンドエイリアスを表示します。

例

すべてのコマンドのエイリアスを表示します。

<AP> display alias

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

コマンドエイリアス shinc を表示します。

<AP> display alias shinc

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

関連コマンド

alias

1.1.7 display history-command

Syntax

display history-command

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display history-command コマンドは履歴バッファに保存されているすべてのコマンドを表示します。このコマンドは現在の CLI セッションで実行された有効なコマンドです。

システムは現在の CLI セッションで実行された有効なコマンドを自動的に保存します。

履歴バッファに保存されているコマンドを表示し、再度実行することができます。

デフォルトで、最大 10 個まで履歴コマンドを保存できます。履歴バッファのサイズを設定するには、**history-command max-size** コマンドを使用します。

バッファサイズが最大のときに新しいコマンドをバッファする場合、システムはバッファのもっとも古いコマンドを削除します。

現在の CLI セッションの履歴コマンドのすべてのコマンドはログアウトしたときに削除されます。

例

現在の CLI セッションで履歴バッファにあるすべてのコマンドを表示します。

<AP> display history-command

```
system-view
vlan 2
quit
```

関連コマンド

history-command max-size

1.1.8 display history-command all

Syntax

display history-command all

View

すべての view

定義済みユーザロール

network-admin

説明

display history-command all コマンドは履歴バッファに保存されているすべてのコマンドを表示します。このコマンドはすべての CLI セッションで実行された有効なコマンドです。

システムはすべてのCLIセッションで実行された有効なコマンドを自動的に保存します。

履歴バッファに保存されているコマンドを表示し、再度実行することができます。

最大 1024 個まで履歴コマンドを保存できます。履歴バッファのサイズが最大になったとき、最初に保存されたコマンドを削除し、新しく実行されたコマンドを保存します。

ユーザがログアウトした場合、すべての CLI セッションの履歴バッファからコマンドを削除します。

例

すべての CLI セッションで履歴バッファにあるすべてのコマンドを表示します。

<AP> display history-command all

```
Date      Time    Terminal   Ip            User
03/16/2017 20:03:33 vty0      192.168.1.26    **
Cmd:dis his all

03/16/2017 20:03:29 vty0      192.168.1.26    **
Cmd:sys
```

表 1-2 コマンド出力

フィールド	説明
Date	コマンドを実行した日付です。
Time	コマンドを実行した時間です。
Terminal	ユーザが使用しているlineです。

フィールド	説明
Ip	ユーザが使用している端末のIPアドレスです。
User	ユーザが使用するユーザ名です。
Cmd	ユーザによって入力したコマンドです。

関連コマンド

display history-command

1.1.9 display hotkey

Syntax

display hotkey

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display hotkey コマンドはホットキー情報を表示します。

例

ホットキー情報を表示します。

<AP> display hotkey

```
----------------- Hotkeys -----------------
         -Defined command hotkeys-
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debugging all
         -undefined command hotkeys-
CTRL_T  NULL
CTRL_U  NULL
         -System-reserved hotkeys-
CTRL_A  Move the cursor to the beginning of the line.
CTRL_B  Move the cursor one character to the left.
CTRL_C  Stop the current command.
CTRL_D  Erase the character at the cursor.
CTRL_E  Move the cursor to the end of the line.
CTRL_F  Move the cursor one character to the right.
CTRL_H  Erase the character to the left of the cursor.
CTRL_K  Abort the connection request.
CTRL_N  Display the next command in the history buffer.
CTRL_P  Display the previous command in the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word to the left of the cursor.
CTRL_X  Delete all characters from the beginning of the line to the cursor.
CTRL_Y  Delete all characters from the cursor to the end of the line.
```

```
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor back one word.
ESC_D   Delete all characters from the cursor to the end of the word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Move the cursor to the beginning of the clipboard.
ESC_>   Move the cursor to the end of the clipboard.
```

関連コマンド

hotkey

1.1.10 hotkey

Syntax

hotkey { CTRL_G | CTRL_L | CTRL_O | CTRL_T | CTRL_U } command

undo hotkey { CTRL_G | CTRL_L | CTRL_O | CTRL_T | CTRL_U }

デフォルト

ctrl_G: **display current-configuration**（カレントコンフィグレーションを表示します。）

ctrl_L: **display ip routing-table**（IPv4 ルーティングテーブル情報を表示します。）

ctrl_O: **undo debugging all**（すべてのデバッグ機能を無効にします。）

ctrl_T: ホットキーにコマンドが割り当てられていません。

ctrl_U: ホットキーにコマンドが割り当てられていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

CTRL_G: ホットキー**Ctrl+G** にコマンドを割り当てます。

CTRL _L: ホットキー**Ctrl+L** にコマンドを割り当てます。

CTRL _O: ホットキー**Ctrl+O** にコマンドを割り当てます。

CTRL _T: ホットキー**Ctrl+T** にコマンドを割り当てます。

CTRL _U: ホットキー**Ctrl+U** にコマンドを割り当てます。

command: ホットキーに割り当てるコマンドを指定します。

説明

hotkey コマンドは設定可能なホットキーにコマンドを割り当てます。

undo hotkey コマンドはデフォルトに戻します。

システムはいくつかのホットキーを定義し、5 つの設定可能なコマンドホットキーを提供します。ホットキーを押下することでホットキーに割り当てられたコマンドを実行します。

システムで定義されたホットキーと設定可能なホットキーを表示するには **display hotkey** コマンドを使用します。

例

ホットキーCTRL+T に **display tcp status** コマンドを割り当てます。

<AP> system-view

[AP] hotkey ctrl_t display tcp statistics

関連コマンド

display hotkey

1.1.11 quit

Syntax

quit

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

quit コマンドは上位の view に戻ります。

user view で **quit** コマンドを実行すると装置から切断されログアウトします。

例

GigabitEthernet 1/0/1 interface view から system view に戻り、次に user view に戻ります。

[AP-GigabitEthernet1/0/1] quit

[AP] quit

<AP>

1.1.12 repeat

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

パラメータ

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

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

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

説明

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

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

対話型コマンドを繰り返す際、システムはユーザの操作を待機します。

パスワード設定コマンドはすべてスキップされます。

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

· repeat コマンドで指定した直近のコマンド数

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

· コマンド履歴バッファ内のコマンド数

例

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

<AP> repeat 2 count 2 delay 10

<AP> display cpu

Unit CPU usage:

33% in last 5 seconds

32% in last 1 minute

33% in last 5 minutes

<AP> display clock

07:02:18 UTC Thu 06/19/2017

<AP> display cpu-usage

Unit CPU usage:

33% in last 5 seconds

32% in last 1 minute

33% in last 5 minutes

<AP> display clock

07:02:28 UTC Thu 06/19/2017

1.1.13 return

Syntax

return

View

user view を除いたすべての view

定義済みユーザロール

network-admin

network-operator

説明

return コマンドはほかの view から user view に戻ります。

Ctrl+Z ホットキーは **return** コマンドと同一です。

例

GigabitEthernet 1/0/1 interface view から user view に戻ります。

[AP-GigabitEthernet1/0/1] return

<AP>

1.1.14 screen-length disable

Syntax

screen-length disable

undo screen-length disable

デフォルト

user line view の **screen-length** コマンドの設定によってデフォルトは変わります。

screen-length コマンドのデフォルトは以下です。

- 出力画面ごとにスクロールを停止します。
- 画面上で一度に 24 行まで表示します。

View

User view

定義済みユーザロール

network-admin

説明

screen-length disable コマンドは現在のセッションで出力画面のスクロールの停止を無効にします。

undo screen-length disable コマンドは現在のセッションで出力画面のスクロールの停止を有効にします。

出力画面のスクロールの停止を無効にした場合、すべての出力が表示されます。最後の画面が表示されるまで連続して画面がリフレッシュします。

本コマンドは現在の画面のみ適用されます。ログアウトすると設定はデフォルトに戻ります。

例

現在のセッションで出力画面のスクロールの停止を無効にします。

<AP> screen-length disable

関連コマンド

screen-length

1.1.15 system-view

Syntax

system-view

View

User view

定義済みユーザロール

network-admin

network-operator

説明

system-view コマンドは user view から system view に移行します。

例

user view から system view に移行します。

<AP> system-view

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

[AP]

目次

このセクションのページは **1-x-x** です。

2 章 ロールベースアクセスコントロール (RBAC)..... 2-1
2.1 ロールベースアクセスコントロール (RBAC) 設定コマンド..... 2-1
2.1.1 description..... 2-1
2.1.2 display role..... 2-2
2.1.3 display role feature..... 2-11
2.1.4 display role feature-group..... 2-14
2.1.5 feature..... 2-16
2.1.6 interface policy deny..... 2-17
2.1.7 permit interface..... 2-18
2.1.8 permit vlan..... 2-20
2.1.9 role..... 2-22
2.1.10 role default-role enable..... 2-24
2.1.11 role feature-group..... 2-25
2.1.12 rule..... 2-26
2.1.13 super..... 2-31
2.1.14 super authentication-mode..... 2-33
2.1.15 super default role..... 2-35
2.1.16 super password..... 2-36
2.1.17 vlan policy deny..... 2-37

2章 ロールベースアクセスコントロール (RBAC)

2.1 ロールベースアクセスコントロール (RBAC) 設定コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

User role view

定義済みユーザロール

network-admin

パラメータ

text: ユーザロールの説明を設定します。設定範囲は 1～128 です。大文字、小文字を区別します。

説明

description コマンドはユーザロールの説明を設定します。

undo description コマンドはユーザロールの説明を削除します。

例

ユーザロール **role1** の説明を **labVIP** に設定します。

<AP> system-view

[AP] role name role1

[AP-role-role1] description labVIP

関連コマンド

- **display role**
- **role**

2.1.2 display role

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *role-name*: ユーザロール名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザロール名を指定しない場合、定義済みのユーザロールを含むすべてのユーザロールの情報を表示します。

説明

display role コマンドはユーザロールの情報を表示します。

例

ユーザロール **123** の情報を表示します。

<AP> display role name 123

```
Role: 123
  Description: new role
  VLAN policy: deny
  Permitted VLANs: 1 to 5, 7 to 8
  Interface policy: deny
  Permitted interfaces: GigabitEthernet1/0/1, Vlan-interface1
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group abc
  2       deny   -W-   feature      ldap
  3       permit       command      system ; radius sc *
  4       permit R--   xml-element   -
  5       permit RW-   oid          1.2.1
  R:Read W:Write X:Execute
```

すべてのユーザロールに関する情報を表示します。

<AP> display role

```
Role: network-admin
  Description: Predefined network admin role has access to all commands on the
device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   permit      command      *
  sys-2   permit RWX   web-menu     -
  sys-3   permit RWX   xml-element   -
  sys-4   deny        command      display security-logfile summary
  sys-5   deny        command      system-view ; info-center
                                 security-logfile directory *
  sys-6   deny        command      security-logfile save
  sys-7   permit RW-   oid          1
  R:Read W:Write X:Execute

Role: network-operator
  Description: Predefined network operator role has access to all read commands
on the device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   permit      command      display *
  sys-2   permit      command      xml
  sys-3   permit      command      system-view ; probe ; display *
  sys-4   deny        command      display history-command all
  sys-5   deny        command      display exception *
  sys-6   deny        command      display cpu-usage configuration
                                 *
  sys-7   deny        command      display kernel exception *
  sys-8   deny        command      display kernel deadloop *
  sys-9   deny        command      display kernel starvation *
  sys-10  deny        command      display kernel reboot *
  sys-13  permit      command      system-view ; local-user *
  sys-15  permit R--   web-menu     -
  sys-16  permit R--   xml-element   -
```

```
  sys-17  deny        command      display security-logfile summary
  sys-18  deny        command      system-view ; info-center
                                  security-logfile directory *
  sys-19  deny        command      security-logfile save
  sys-20  deny        command      system-view ; local-user-import
                                  *
  sys-21  deny        command      system-view ; local-user-export
                                  *
  sys-22  permit R--   oid          1
  sys-23  deny        command      display smartmc *
  R:Read W:Write X:Execute

Role: level-0
  Description: Predefined level-0 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope        Entity
  ----------------------------------------------------------------------
  sys-1   permit      command      tracert *
  sys-2   permit      command      telnet *
  sys-3   permit      command      ping *
  sys-4   permit      command      ssh2 *
  sys-5   permit      command      super *
  sys-6   permit      command      mtrace *
  R:Read W:Write X:Execute

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

```
  sys-8   permit      command      mtrace *
  R:Read W:Write X:Execute

Role: level-2
  Description: Predefined level-2 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

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

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

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

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

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

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

```
  VPN instance policy: permit (default)

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

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

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

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

Role: level-13
  Description: Predefined level-13 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)

Role: level-14
  Description: Predefined level-14 role
```

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

Role: level-15
  Description: Predefined level-15 role
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   permit      command     *
  sys-2   permit RWX   web-menu     -
  sys-3   permit RWX   xml-element   -
  sys-4   deny        command     display security-logfile summary
  sys-5   deny        command     system-view ; info-center
                                security-logfile directory *
  sys-6   deny        command     security-logfile save
  sys-7   permit RW-   oid         1
  sys-8   deny        command     display smartmc *
  sys-9   deny        command     debugging smartmc *
  sys-10  deny        command     undo debugging smartmc *
  sys-11  deny        command     system-view ; smartmc *
  sys-12  deny        command     system-view ; undo smartmc *
  sys-13  deny        command     system-view ; interface * ; smartmc *
  sys-14  deny        command     system-view ; interface * ; undo
                                 smartmc *
  sys-29  deny        command     create batch-file *
  R:Read W:Write X:Execute

Role: security-audit
  Description: Predefined security audit role only has access to commands for the
security log administrator
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope       Entity
  ----------------------------------------------------------------------
  sys-1   deny        command     *
  sys-2   permit      command     display security-logfile summary
  sys-3   permit      command     system-view ; info-center
```

```
                                security-logfile directory *
  sys-4   permit      command      security-logfile save
  sys-5   permit      command      cd *
  sys-6   permit      command      copy *
  sys-7   permit      command      delete *
  sys-8   permit      command      dir *
  sys-9   permit      command      mkdir *
  sys-10  permit      command      more *
  sys-11  permit      command      move *
  sys-12  permit      command      rmdir *
  sys-13  permit      command      pwd
  sys-14  permit      command      rename *
  sys-15  permit      command      undelete *
  sys-16  permit      command      ftp *
  sys-17  permit      command      sftp *
  R:Read W:Write X:Execute

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

表 2-1 コマンド出力

フィールド	説明
Role	ユーザロール名です。 定義済みのユーザロール名は以下です。 ● network-admin ● network-operator ● level-*n*（*n*は0～15の整数です） ● security-audit. ● guest-manager.
Description	設定内容を容易に識別できるようにするためのユーザロールの説明です。
VLAN policy	ユーザロールのVLANポリシーです。 ● **deny**–許可されたVLANを除くVLANへのアクセスを拒否します。 ● **permit (default)**–デフォルトVLANポリシーです。すべてのVLANにアクセスするユーザロールを有効にします。
Permitted VLANs	ユーザロールにアクセス可能なVLANです。
Interface policy	ユーザロールのインタフェースポリシーです。 ● **deny**–許可されたインタフェースを除くインタフェースへのアクセスを拒否します。 ● **permit (default)**–デフォルトインタフェースポリシーです。すべてのインタフェースにアクセスするユーザロールを有効にします。
Permitted interfaces	ユーザロールにアクセス可能なインタフェースです。
VPN instance policy	ユーザロールのVPNインスタンスポリシーです。 ● **deny**–許可されたVPNインスタンスを除くVPNインスタンスへのアクセスを拒否します。 ● **permit (default)**–デフォルトVPNインスタンスポリシーです。すべてのVPNインスタンスにアクセスするユーザ ロールを有効にします。
Permitted VPN instances	ユーザロールにアクセス可能なVPNインスタンスです。
Rule	ユーザロール番号です。 定義済みのユーザロールのルールはsys-*n*で指定されます。 ここで*n*は整数です。

フィールド	説明
Perm	アクセス制御タイプです。 ● **permit**–ユーザロールは、**Entity**フィールドの項目にアクセスできます。 ● **deny**–ユーザロールは、**Entity**フィールドの項目にアクセスできません。
Type	制御タイプです。 ● **R**–Read-onlyです。 ● **W**–Writeです。 ● **X**–Executeです。
Scope	ルール制御範囲です。 ● **command**–コマンドへのアクセスを制御する、あるいは**Entity**フィールドで指定されるコマンドです。 ● **feature**–**Entity**フィールドに指定され、機能のコマンドへのアクセスを制御します。 ● **feature-group**–**Entity**フィールドに指定され、機能グループの機能のコマンドへのアクセスを制御します。 ● **web-menu**–Webメニューへのアクセスを制御します。このルール制御範囲は、現在のソフトウェアバージョンではサポートされていません。 ● **xml-element**—XML要素へのアクセスを制御します。 ● **oid**–MIBノードへのアクセスを制御します。
Entity	ユーザグループルールで指定されたコマンド文字列、機能名、機能グループです。 ● エンダッシュ（–）はすべての機能を示します。 ● アスタリスク（*）は0以上の文字を示します。

関連コマンド

role

2.1.3 display role feature

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *feature-name*: 機能のコマンドを表示します。*feature-name* は機能名を指定します。すべての文字は小文字にする必要があります。

verbose: 各機能のコマンドを表示します。

説明

display role feature コマンドはシステムで有効な機能を表示します。

パラメータを指定しない場合、システムで有効な機能のリストのみを表示します。

例

機能のリストを表示します。

<AP> display role feature

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

...

各機能のコマンドを表示します。

<AP> display role feature verbose

```
Feature: device         (Device configuration related commands)
  display clock    (R)
  debugging dev    (W)
  display debugging dev    (R)
  display device *    (R)
  display diagnostic-information *    (R)
  display environment *    (R)
  display fan *    (R)
  display power *    (R)
```

```
  display current-configuration *    (R)
  display saved-configuration *    (R)
  display default-configuration *    (R)
  display startup    (R)
  display this *    (R)
...
```

 # aaa 機能のコマンドを表示します。

<AP> display role feature name aaa

```
Feature: aaa            (AAA related commands)
  system-view ; domain *    (W)
  system-view ; header *    (W)
  system-view ; aaa *    (W)
  display domain *    (R)
  display aaa *    (R)
  system-view ; user-group *    (W)
  system-view ; local-user *    (W)
  display local-user *    (R)
  display user-group *    (R)
  display debugging local-server    (R)
  debugging local-server *    (W)
  super *    (X)
  display password-control *    (R)
  reset password-control *    (W)
  system-view ; password-control *    (W)
...
```

表 2-2 コマンド出力 (**display role feature name** *aaa*)

フィールド	説明
Feature	機能の名前、概要の説明を表示します。
system-view ; domain *	system viewでの**domain**キーワードで始まるすべてのコマンドです。ISP domain viewでのすべてのコマンドです。
system-view ; header *	system viewでの**header**キーワードで始まるすべてのコマンドです。
system-view ; aaa *	system viewでの**aaa**で始まるすべてのコマンドです。
display domain *	user viewでの**display domain**キーワードで始まるすべてのコマンドです。
system-view ; user-group *	system viewでの**user-group**キーワードで始まるすべてのコマンドとuser group viewのすべてのコマンドです。
system-view ; local-user *	system viewでの**local-user**キーワードで始まるすべてのコマンドとlocal user viewのすべてのコマンドです。

フィールド	説明
display user-group *	user viewでの**display user-group**キーワードで始まるすべてのコマンドです。
display debugging local-server	user viewでの**display debugging local-server**キーワードで始まるすべてのコマンドです。
debugging local-server *	user viewでの**debugging local-server**キーワードで始まるすべてのコマンドです。
super *	user viewでの**super**キーワードで始まるすべてのコマンドです。
display password-control *	user viewでの**display password-control**キーワードで始まるすべてのコマンドです。
reset password-control *	user viewでの**reset password-control**キーワードで始まるすべてのコマンドです。
system-view ; password-control *	system viewでの**password-control**キーワードで始まるすべてのコマンドです。
(W)	コマンドタイプがwriteです。writeコマンドはシステムを設定します。
(R)	コマンドタイプがreadです。readコマンドは設定を表示あるいは情報を維持します。
(X)	コマンドタイプがexecuteです。execute コマンドは指定した機能を実行します。

関連コマンド

feature

2.1.4 display role feature-group

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *feature-group-name*: 機能グループを指定します。*feature-group-name* は機能グループ名を指定します。設定範囲は 1～31 です。大文字、小文字を区別します。機能グループを指定しない場合、すべての機能グループの情報を表示します。

verbose: 指定された機能グループの各機能のコマンドを表示します。機能グループを指定しない場合、各機能グループの各機能のコマンドを表示します。**verbose** キーワードを指定しない場合、機能グループの機能リストのみを表示します。

説明

display role feature-group コマンドは機能グループの情報を表示します。

機能グループ **L2**、**L3** は機能グループで定義されています。

例

機能グループの機能リストを表示します。

<AP> display role feature-group

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

Feature group: L3
Feature: route          (Route management related commands)
Feature: usr            (Unicast static route related commands)
```

```
Feature: l3vpn          (Layer 3 Virtual Private Network related commands)
Feature: multicast      (Multicast related commands)
```

各機能グループのコマンドを表示します。コマンドのワイルドカードと記号についての詳細は、表 2-2 を参照してください。

<AP> display role feature-group verbose

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

機能グループ **L3** の機能リストを表示します。

<AP> display role feature-group name L3

```
Feature group: L3
Feature: route          (Route management related commands)
Feature: usr           (Unicast static route related commands)
Feature: l3vpn          (Layer 3 Virtual Private Network related commands)
Feature: multicast      (Multicast related commands)
```

関連コマンド

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

2.1.5 feature

Syntax

feature *feature-name*

undo feature *feature-name*

デフォルト

設定なし

View

Feature group view

定義済みユーザロール

network-admin

パラメータ

feature-name: 機能名を指定します。機能名は小文字で入力する必要があります。

説明

feature コマンドは機能グループに機能を追加します。

undo feature コマンドは機能グループから機能を削除します。

機能グループに複数の機能を追加する場合、**feature** コマンドを繰り返してください。

例

セキュリティグループ **security-features** にセキュリティ機能 AAA、ACL を追加します。

<AP> system-view

[AP] role feature-group name security-features

[AP-featuregrp-security-features] feature aaa

[AP-featuregrp-security-features] feature acl

関連コマンド

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

2.1.6 interface policy deny

Syntax

interface policy deny

undo interface policy deny

デフォルト

User role はすべてのインタフェースにアクセスできます。

View

User role view

定義済みユーザロール

network-admin

説明

interface policy deny コマンドはインタフェースへのアクセスを拒否し、ユーザロールの interface policy view に移行します。

undo interface policy deny コマンドはユーザロールインタフェースポリシーをデフォルトに戻します。

指定したインタフェースのみユーザロールのインタフェースへのアクセスを制限するために、以下の作業を行います。

1) **interface policy deny** コマンドでユーザロールインタフェースポリシーview に移行します。
2) **permit interface** コマンドでアクセス可能なインタフェースを指定します。

🕮 **メモ**:

interface policy deny コマンドは、**permit interface** コマンドが設定されていない場合、すべてのインタフェースへのユーザロールのアクセスを拒否します。

インタフェースを設定するため、ユーザロールのインタフェースポリシーで許可されているインタフェースが使用されているであることを確認してください。アクセス可能なインタフェースで以下の操作を実行することができます。

- インタフェースの作成、削除、設定を行います。
- interface view へ移行します。
- **feature** コマンドでインタフェースを指定します。

作成および削除は、論理インタフェースでのみ有効です。

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

例

ユーザロール **role1** でインタフェースへのアクセスを拒否します。

<AP> system-view

[AP] role name role1

[AP-role-role1] interface policy deny

[AP-role-role1-ifpolicy] quit

関連コマンド

- **display role**
- **permit interface**
- **role**

2.1.7 permit interface

Syntax

permit interface *interface-list*

undo permit interface [*interface-list*]

デフォルト

ユーザロールの interface policy view で許可されているインタフェースはありません。

View

User role interface policy view

定義済みユーザロール

network-admin

パラメータ

interface *interface-list*: 最大 10 個のインタフェース項目をスペースで区切り、リストを指定することができます。各インタフェースは *interface-type interface-number* あるいは *interface-type interface-number* **to** *interface-type interface-number* の形式で指定します。インタフェースの範囲を指定する場合、終了インタフェースは以下の要件に一致する必要があります。

- 開始インタフェースと同一のタイプにしてください。
- 開始インタフェースよりもインタフェース番号を大きい値にしてください。

説明

permit interface コマンドはユーザロールにアクセス可能なインタフェースのリストを設定します。

undo permit interface コマンドは指定したインタフェースのアクセスを無効にします。

interface policy deny コマンドを設定した後、インタフェースにアクセスするユーザロールを許可するため、ポリシーの許可されたインタフェースリストにインタフェースを追加する必要があります。ユーザロールで許可されたインタフェースリストのインタフェースで以下の操作を実行することができます。

- インタフェースの作成、削除、設定を行います。
- interface view へ移行します。
- **feature** コマンドでインタフェースを指定します。

作成および削除は、論理インタフェースでのみ有効です。

ユーザロールのインタフェースポリシーに許可されたインタフェースを追加するため、**permit interface** コマンドを複数繰り返すことができます。

インタフェースを指定しない場合、**undo permit interface** コマンドは許可されたインタフェースのリスト全体を削除します。

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

例

1)　ユーザロール **role1** を設定します。

interface view、VLAN view で有効なすべてのコマンドを実行するため、ユーザロール **role1** を許可します。

<AP> system-view

[AP] role name role1

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

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

GigabitEthernet 1/0/1、GigabitEthernet 1/0/3～GigabitEthernet 1/0/5 へアクセスするため、ユーザロールを許可します。

[AP-role-role1] interface policy deny

[AP-role-role1-ifpolicy] permit interface GigabitEthernet 1/0/1 GigabitEthernet 1/0/3 to GigabitEthernet 1/0/5

[AP-role-role1-ifpolicy] quit

[AP-role-role1] quit

2)　ユーザロール **role1** で GigabitEthernet 1/0/1、GigabitEthernet 1/0/3～GigabitEthernet 1/0/5 を除いたインタフェースで動作するユーザロールが使用できないことを確認します。

GigabitEthernet 1/0/1 interface view に移行できることを確認します。

[AP] interface GigabitEthernet 1/0/1

[AP-GigabitEthernet1/0/1] quit

GigabitEthernet 1/0/5 に VLAN 10 の割り当てができることを確認します。この例では、ユーザロールのデフォルト VLAN ポリシーが使用されているため、ユーザロールはすべての VLAN にアクセスできます。

[AP] vlan 10

[AP-vlan10] port GigabitEthernet 1/0/5

[AP-vlan10] quit

GigabitEthernet 1/0/2 の interface view に移行できないことを確認します。

[AP] interface GigabitEthernet 1/0/2

```
Permission denied.
```

関連コマンド

- **display role**
- **interface policy deny**
- **role**

2.1.8 permit vlan

Syntax

permit vlan *vlan-id-list*

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

デフォルト

ユーザロールの VLAN policy view で許可されている VLAN の設定はありません。

View

User role VLAN policy view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切ることで 10 の VLAN を指定することができます。

各 VLAN は VLAN ID で VLAN を指定あるいは *vlan-id1* **to** *vlan-id2* の形式で指定します。VLAN ID の設定範囲は 1～4094 です。VLAN の範囲を指定する場合、*vlan-id2* は *vlan-id1* よりも大きい値にしてください。

説明

permit vlan コマンドはユーザロールにアクセスできる VLAN のリストを設定します。

undo permit vlan コマンドは指定した VLAN にアクセスするため、ユーザロールの許可を削除します。

vlan policy deny コマンドを設定したのち、VLAN にアクセスするユーザロールを許可するために、ポリシーの許可された VLAN リストに VLAN を追加する必要があります。ユーザロールで、許可された VLAN リストの VLAN で以下の操作を実行することができます。

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

ユーザロールの VLAN ポリシーに許可された VLAN を追加するため、**permit vlan** コマンドを複数繰り返すことができます。

VLAN を指定しない場合、**undo permit vlan** コマンドは許可された VLAN のリスト全体を削除します。

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

デフォルトでは、すべてのアクセスポートは VLAN 1 に属します。

port access vlan コマンドを使用してアクセスポートを他のすべての VLAN に割り当てるには、VLAN 1 と新しい VLAN の両方にアクセスできるユーザロールがあることを確認します。

例

1)　ユーザロール **role1** を設定します。

interface view、VLAN view で有効なすべてのコマンドを実行するため、ユーザロール **role1** を許可します。

<AP> system-view

[AP] role name role1

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

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

VLAN 1、VLAN 2、VLAN 4、VLAN 50～VLAN 100 にアクセスするユーザロール **role1** を許可します。

[AP-role-role1] vlan policy deny

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

[AP-role-role1-vlanpolicy] quit

[AP-role-role1] quit

2)　VLAN 1、VLAN 2、VLAN 4、VLAN 50～VLAN 100 を除いた VLAN で動作するユーザロール **role1** が使用できないことを確認します。

VLAN 100 を作成し、VLAN view に移行できることを確認します。

[AP] vlan 100

[AP-vlan100] quit

アクセスポートとして VLAN 100 に GigabitEthernet 1/0/1 を追加できることを確認します。

[AP] interface GigabitEthernet 1/0/1

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

[AP-GigabitEthernet1/0/1] quit

VLAN 101 を作成し、VLAN view に移行できないことを確認します。

[AP] vlan 101

```
Permission denied.
```

関連コマンド

- **display role**
- **role**
- **vlan policy deny**

2.1.9 role

Syntax

role name *role-name*

undo role name *role-name*

デフォルト

以下の定義済みユーザロールがあります。

- network-admin
- network-operator
- level-*n*（*n* は 0～15 の整数です）

View

System view

定義済みユーザロール

network-admin

パラメータ

name *role-name*: ユーザ名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

説明

role コマンドはユーザロールを作成し、user role view に移行します。ユーザロールが作成されている場合、直接 user role view に移行します。

undo role コマンドはユーザロールを削除します。

定義済みのユーザロールに加えて 64 のユーザロールを作成することができます。

定義済みのユーザロールを削除することはできません。あるいは定義済みの network-admin、network-operator、level-15 に割り当てられた許可を変更することはできません。

非 AAA 認証ユーザにセキュリティ検査のロールを割り当てることはできません。

Level-0～level-14 のユーザロールのアクセス許可は、ユーザロールのルールとリソースのアクセスポリシーを使用して変更できます。

ただし、これらのユーザロールの定義済みアクセス権を変更することはできません。

これらのユーザロールのアクセス権を **display history-command all** コマンドに変更することはできません。

例

ユーザロール **role1** を作成し、user role view に移行します。

<AP> system-view

[AP] role name role1

[AP-role-role1]

関連コマンド

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

2.1.10 role default-role enable

Syntax

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

undo role default-role enable

デフォルト

デフォルトユーザロール機能は無効です。ユーザロールがない AAA ユーザは装置にログインすることができません。

View

System view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。ユーザロールはシステムになければなりません。ユーザロールの指定がない場合、デフォルトユーザロールとしてコマンドは network-operator を指定します。

説明

role default-role enable コマンドはリモート AAA ユーザのデフォルトユーザロールを有効にします。

undo role default-role enable コマンドはデフォルトに戻します。

AAA サーバがユーザにすべてのユーザロールを許可しない場合、デフォルトユーザロール機能は AAA 認証ユーザにデフォルトユーザロールを割り当てます。これらのユーザは、デフォルトユーザロールでシステムへのアクセスが許可されます。

ローカル認証では、**authorization-attribute user role** コマンドを使用して、ユーザロールをローカルユーザに割り当てない場合、このコマンドが必要です。

AAA ユーザにユーザロールが割り当てられている場合、ユーザロールでログインします。

例

デフォルトユーザロール機能を有効にします。

<AP> system-view

[AP] role default-role enable

関連コマンド

role

2.1.11 role feature-group

Syntax

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

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

デフォルト

ユーザロールグループ **L2**、**L3** が作成されています。

View

System view

定義済みユーザロール

network-admin

パラメータ

name *feature-group-name*: 機能グループ名を指定します。設定範囲は 1～31 です。大文字、小文字を区別します。

説明

role feature-group コマンドはユーザロール機能グループを作成し、ユーザロールの group view に移行します。

undo role feature-group コマンドはユーザロール機能グループを削除します。

L2 機能グループはすべてのレイヤ 2 機能コマンドを含みます。**L3** 機能グループはすべてのレイヤ 3 機能コマンドを含みます。この定義済みの機能グループはユーザが設定できません。

定義済みの機能グループ **L2**、**L3** に加えて、64 のユーザ機能グループを作成することができます。

例

機能グループ **security-features** を作成し、その view に移行します。

<AP> system-view

[AP] role feature-group name security-features

[AP-featuregrp-security-features]

関連コマンド

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

2.1.12 rule

Syntax

rule *number* { **deny** | **permit** } { **command** *command-string* | { **execute** | **read** | **write** } * { **feature** [*feature-name*] | **feature-group** *feature-group-name* |

web-menu [web-string] | **xml-element** [xml-string] } }

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

デフォルト

ユーザが定義したユーザロールにルールがなく、すべてのコマンドへのアクセスができません。

View

User role view

定義済みユーザロール

network-admin

パラメータ

number: ルール番号を指定します。設定範囲は 1～256 です。

deny: 指定されたコマンドへのアクセスを拒否します。

permit: 指定されたコマンドへのアクセスを許可します。

command *command-string*: コマンドを指定します。*command-string* の設定範囲は 1～128 です。大文字、小文字を区別します。以下の記号を含むことができます。

- ワイルドカードアスタリスク(*)
- 半角スペースとタブキーの区切り記号
- 印刷可能な文字列

execute: 実行コマンドを指定します。**execute** コマンドは指定した機能あるいはプログラムを実行します。たとえば **ping** コマンドです。

read: 読み込みコマンドを指定します。**read** コマンドは設定を表示あるいは情報を維持します。たとえば、**display、dir、more、pwd** コマンドです。

write: 書き込みコマンドを指定します。**write** コマンドはシステムを設定します。たとえば、**ssh server enable** コマンドです。

feature [*feature-name*]: 1 つ以上の機能を指定します。*feature-name* は機能名を指定します。機能名を指定しない場合、システムのすべての機能を指定します。機能を指定するとき、機能名は **display role feature** コマンドで表示される名前と同一にしてください。

feature-group *feature-group-name*: ユーザ定義あるいは定義済みの機能グループを指定します。*feature-group-name* は機能グループ名を示します。設定範囲は 1～31 です。大文字、小文字を区別します。機能グループが作成されていない場合、ルールはグループ

が作成されたのち適用されます。作成された機能グループを表示する場合、**display role feature-group** コマンドを使用します。

web-menu [web-string]: Web メニューを指定します。web-string 引数は、Web メニューの ID パスを表し、大文字と小文字を区別しない 1 ～ 255 文字の文字列です。

M_DEVICE/I_BASIC_INFO/I_reboot のように、スラッシュ (/) を使用して ID 項目を区切ります。Web メニューを指定しない場合、ルールはすべての Web アイテムに適用されます。Web メニューの ID パスを確認するには、display web menu コマンドを使用します。

xml-element [xml-string]: XML エレメントを指定します。xml-string 引数は、XML エレメントの XPath を表し、大文字と小文字を区別しない 1 ～ 255 文字の文字列です。

Interfaces/Index/Name など、スラッシュ (/) を使用して Xpath 項目を区切ります。

XML エレメントを指定しない場合､ルールはすべての XML エレメントに適用されます。

all: すべてのユーザロールのルールを削除します。

説明

rule コマンドは制御するコマンドのユーザロールのルールを作成あるいは変更します。

undo rule コマンドはユーザロールのルールを削除します。

細分化された異なるアクセス制御を行うため、以下のルールのタイプを定義することができます。

- **Command rule**－正規表現に一致するコマンドあるいはコマンドリストへのアクセス制御を行います。
- **Feature rule**－コマンドタイプによって機能のコマンドにアクセス制御を行います。
- **Feature group rule**－コマンドタイプによって機能グループのコマンドにアクセス制御を行います。
- **Web menu rule**－メニュータイプごとに Web メニューへのアクセスを制御します。
- **XML element rule**－要素タイプ別に XML 要素へのアクセスを制御します。

ユーザロールは、ユーザロールルールで指定されている許可されたリソースのセットにアクセスできます。

ユーザロールルールには、定義済み（sys-n で識別）およびユーザ定義のユーザロールルールが含まれます。

ユーザロールには最大 256 のユーザ定義ルールを設定できます。

ユーザ定義ユーザロールルールの総数は 1024 以下です。

ユーザロールに対するルールの変更、追加、または削除は、変更後にそのユーザロールでログインしたユーザにのみ有効になります。

ファイルシステムコマンドへのアクセスは、ファイルシステムコマンドルールとファイルシステム機能ルールの両方によって制御されます。

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

以下のガイドラインは、OID 以外のルールに適用されます。

- 同一タイプのユーザ定義のルールが混在した場合、高いIDのルールが適用されます。たとえば、もしユーザロールに以下のコマンドを使用したルールが含まれる場合、ユーザロールが **tracert** コマンドを使用することができますが、**ping** コマンドは使用できません。
  - **rule** *1* **permit command** *ping*
  - **rule** *2* **permit command** *tracert*
  - **rule** *3* **deny command** *ping*
- 定義済みのユーザロールのルールとユーザ定義のユーザロールが混在した場合、ユーザ定義したユーザロールが適用されます。

コマンド文字列を指定するとき、表 2-3 のガイドラインに従ってください。

表 2-3 コマンド文字列設定ルール

ルール	ガイドライン
区切り機能はセミコロン（;）です。	コマンドあるいはコマンドリストにアクセスする前に、各viewのコマンドを区切るためにセミコロンを使用してください。しかし**display**コマンドや**dir**コマンドなどuser viewやすべてのviewで有効なコマンドを区切るためにセミコロンを使用しないでください。 セミコロンで区切られたセグメントは、最小限、印刷可能な1文字がある必要があります。 viewにあるが、サブviewにないコマンドを指定する場合、最後のセグメントの最後の印刷可能な文字にセミコロンを使用してください。viewとviewのサブviewにあるコマンドを指定する場合、最後のセグメントの最後の印刷可能な文字にセミコロンを使用しないでください。 たとえば、interface viewに移行する前にsystem viewに移行してください。すべてのinterface viewの**ip**キーワードで開始するすべてのコマンドを指定するため、**system ; interface * ; ip * ;**を使用してください。 **system ; radius scheme * ;**コマンドはsystem viewの**radius scheme**キーワードで始まるすべてのコマンドを示します。 **system ; radius scheme ***コマンドはsystem viewの**radius scheme**キーワードで始まるすべてのコマンドとRADIUS scheme viewのすべてのコマンドを示します。
アスタリスクがワイルドカードです。	アスタリスクは0あるいは複数の文字を示します。 最後のセグメントでない場合、セグメントの最後のみアスタリスクを使用することができます。 最後のセグメントである場合、セグメントのいずれの位置でもアスタリスクを使用することができます。アスタリスクから始まる場合、アスタリスクの後ろに印刷可能な文字を指定することができません。 たとえば、**system ; ***コマンドはsystem viewとsystem viewのサブ

ルール	ガイドライン
	viewで有効なすべてのコマンドを示します。**debugging * event** コマンドはuser viewで有効なすべてのイベントをデバッグするコマンドを示します。
キーワードの省略ができます。	キーワードの最初の数文字を入力することでキーワードを指定することができます。ルールに一致する文字列から始まるすべてのコマンドです。 たとえば、**rule 1 deny command dis arp source *** コマンドは **display arp source-mac interface** コマンドと **display arp source-suppression.** コマンドのアクセスを拒否します。
コマンドへのアクセスを制御するため、コマンドがあるviewの直後にコマンドを指定する必要があります。	コマンドへのアクセスを制御するため、コマンドが割り当てられたviewの直後にコマンドを指定する必要があります。すべてのサブviewのコマンドを制御するルールはコマンドに適用されません。 たとえば、**rule 1 deny command system ; interface * ; *** コマンドはinterface viewに割り当てられたコマンドへのアクセスを無効にします。しかしこのコマンドはsystem viewよりもinterface viewで割り当てられるため、interface viewの **acl advanced** コマンドを実行することができます。 このコマンドへのアクセスを無効にする場合、**rule 1 deny command system ; acl *;** コマンドを使用します。
ユーザロールのコマンドルールの **display** コマンドを指定するとき、垂直バー（|）、大なり記号（>）、2重大なり記号（>>）を含みません。	システムはコマンドラインの一部として記号に従うリダイレクト記号とパラメータを含みません。 ユーザロールのコマンドルールで、コマンドラインの一部にリダイレクト記号とパラメータが存在します。その結果、これらの記号を含むルールは一致するコマンドはありません。 たとえば、**rule 1 permit command display debugging > log** コマンドは、**display debugging** コマンドではなく、**display debugging > log** コマンドに一致するコマンドはありません。

例

display acl コマンドを実行するユーザロール **role1** を許可します。

<AP> system-view

[AP] role name role1

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

display キーワードで開始するすべてのコマンドを実行するユーザロール **role1** を許可します。

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

system view の **radius scheme aaa** コマンドを実行するユーザロール **role1** を許可し、RADIUS scheme view に割り当てられたすべてのコマンドを使用します。

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

すべての機能の read あるいは write コマンドへアクセスするユーザロール **role1** を拒否します。

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

aaa 機能のすべての read コマンドへアクセスするユーザロール **role1** を拒否します。

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

機能グループ **security-features** の read、write、execute コマンドへアクセスするユーザロール **role1** を許可します。

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

関連コマンド

- **display role**
- **display role feature**
- **display role feature-group**
- **display web menu**
- **role**

2.1.13 super

Syntax

super [*role-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があります。ユーザロールを指定しない場合、デフォルトターゲットのユーザロールを取得します。

説明

super コマンドは装置に再接続することなく、別のユーザロールを取得します。

このコマンドは現在のログインでのみ適用されるため、取得されたユーザロールは一時的なユーザロールです。次回ユーザアカウントでログインすると、元のユーザロールの設定が適用されます。

装置に再接続することなく、ユーザが別のユーザロールを取得するため、ユーザロールの認証を設定する必要があります。

- ローカルパスワードがローカルパスワード認証（**local**）で設定されていない場合、AUX ユーザはいずれかの文字列を入力するか、なにも入力しないことでユーザロールの許可を取得できます。
- ローカルパスワードが local-then-remote 認証（**local scheme**）で設定されていない場合、以下のルールが適用されます。
  - VTY ユーザはリモート認証を実行します。
  - AUX ユーザはいずれかの文字列を入力するか、なにも入力しないことでユーザロールの許可を取得できます。

例

ユーザロール network-operator を取得します。

<AP> super network-operator

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

関連コマンド

- **authentication super**(コマンドマニュアルのセクション 13 *セキュリティ*)

- **super authentication-mode**
- **super password**

2.1.14 super authentication-mode

Syntax

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

undo super authentication-mode

デフォルト

local

View

System view

定義済みユーザロール

network-admin

パラメータ

local: ローカルパスワード認証を有効にします。

scheme: リモート AAA 認証を有効にします。

説明

super authentication-mode コマンドは一時的なユーザロールの許可を取得するため認証モードを設定します。

undo super authentication-mode コマンドはデフォルトに戻します。

ローカルパスワードでは、パスワードを設定するため、**super password** コマンドを使用します。

リモート AAA 認証では、RADIUS サーバのユーザ名とパスワードを設定します。

local と **scheme** キーワードの両方を指定した場合、最初に指定されたキーワードが適用されます。

- **scheme local**−remote-then-local 認証モードを有効にします。装置は一時的なユーザロールを取得するため、最初に AAA 認証を実行します。リモート RADIUS サーバが応答しないあるいは装置の AAA の設定が無効である場合、ローカル認証が実行されます。
- **local scheme**−local-then-remote 認証モードを有効にします。装置は最初にローカルパスワード認証を実行します。ユーザロールのパスワードが設定されていない場合、装置はリモート認証を実行します。VTY ユーザ、AUX ユーザは、文字列を入力するか、何も入力しないで別のユーザロールを取得できます。

AAA の詳細は、オペレーションマニュアルのセクション 12 *ユーザアクセスの認証 "AAA"* を参照してください。

例

一時的なユーザロールの許可を取得するため、local-only 認証を有効にします。

<AP> system-view

[AP] super authentication-mode local

一時的なユーザロールの許可を取得するため、remote-then-local 認証を有効にします。

<AP> system-view

[AP] super authentication-mode scheme local

関連コマンド

- **authentication super**(コマンドマニュアルのセクション 13 *セキュリティ*)
- **super password**

2.1.15 super default role

Syntax

super default role *role-name*

undo super default role

デフォルト

network-admin

View

System view

定義済みユーザロール

network-admin

パラメータ

role-name: デフォルトターゲットユーザロールの名前を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があり、セキュリティ監査になることはできません。

説明

super default role コマンドは一時的なユーザロールの許可を取得するためデフォルトターゲットのユーザロールを指定します。

undo super default role コマンドはデフォルトに戻します。

コマンドのユーザロールを指定しないとき、デフォルトターゲットのユーザロールが **super** コマンドあるいは **super password** コマンドに割り当てられます。

例

一時的なユーザロールの許可を取得するため、デフォルトターゲットのユーザロールを **network-operator** に指定します。

<AP> system-view

[AP] super default role network-operator

関連コマンド

- **super**
- **super password**

2.1.16 super password

Syntax

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

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

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

role *role-name*: ユーザロールを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。システムにユーザロールが存在する必要があり、セキュリティ監査にはなれません。ユーザロールを指定しない場合、**super default role** コマンドを使用して設定される、デフォルトターゲットのユーザロールのパスワードを設定します。

hash: ハッシュテキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、ハッシュテキストで保存され、暗号化されます。

string: パスワードを指定します。大文字、小文字を区別します。

- **simple** キーワードが指定される場合、パスワードの設定範囲は 1～63 文字です。
- **hash** キーワードが指定される場合、パスワードの設定範囲は 1～110 文字です。

説明

super password コマンドはユーザロールのパスワードを設定します。

undo super password コマンドはデフォルトに戻します。

パラメータを指定しない場合、インタラクティブモードでプレーンテキストパスワードを指定します。

一時的なユーザロールの許可のローカルパスワード認証を設定する場合、パスワードを設定します。

異なるユーザロールに異なるパスワードを指定することを推奨します。

例

ユーザロール network-operator のプレーンテキストのパスワード **123456TESTplat&!** を設定します。

<AP> system-view

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

ユーザロール network-operator のパスワード **123456TESTplat&!**をインタラクティブモードで設定します。

<AP> system-view

[AP] super password role network-operator

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

関連コマンド

- **super authentication-mode**
- **super default role**

2.1.17 vlan policy deny

Syntax

vlan policy deny

undo vlan policy deny

デフォルト

VLAN へのユーザロールのアクセス可能にします。

View

User role view

定義済みユーザロール

network-admin

説明

vlan policy deny コマンドは VLAN へのユーザロールのアクセスを拒否し、ユーザロールの VLAN policy view に移行します。

undo vlan policy deny コマンドはユーザロールの VLAN policy view へのアクセスをデフォルトに戻します。

指定した VLAN のみユーザロールの VLAN へのアクセスを制限するために、以下の作業を行います。

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

🕮 **メモ：**

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

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

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

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

例

VLAN へのユーザロール **role1** のアクセスを拒否します。

<AP> system-view

[AP] role name role1

[AP-role-role1] vlan policy deny

[AP-role-role1-vlanpolicy] quit

VLAN50～VLAN100 を除く VLAN へのユーザロール **role1** のアクセスを拒否します。

<AP> system-view

[AP] role name role1

[AP-role-role1] vlan policy deny

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

関連コマンド

- **display role**
- **permit vlan**
- **role**

目次

このセクションのページは **1-x-x** です。

3 章 ログイン 3-1
3.1 ログイン設定 3-1
3.1.1 authentication-mode 3-2
3.1.2 auto-execute command 3-4
3.1.3 display ip http 3-5
3.1.4 display ip https 3-6
3.1.5 display line 3-8
3.1.6 display user-interface 3-10
3.1.7 display users 3-12
3.1.8 display web menu 3-14
3.1.9 display web users 3-15
3.1.10 escape-key 3-16
3.1.11 free line 3-19
3.1.12 free user-interface 3-20
3.1.13 free web users 3-22
3.1.14 history-command max-size 3-23
3.1.15 idle-timeout 3-24
3.1.16 ip http acl 3-25
3.1.17 ip http enable 3-27
3.1.18 ip http port 3-28
3.1.19 ip https acl 3-29
3.1.20 ip https enable 3-30
3.1.21 ip https port 3-32
3.1.22 line 3-32
3.1.23 line class 3-34
3.1.24 lock 3-36
3.1.25 protocol inbound 3-36
3.1.26 screen-length 3-38
3.1.27 send 3-40
3.1.28 set authentication password 3-41
3.1.29 shell 3-43
3.1.30 telnet server acl 3-44
3.1.31 telnet server acl-deny-log enable 3-45
3.1.32 telnet server dscp 3-46
3.1.33 telnet server enable 3-47
3.1.34 telnet server port 3-48

3.1.35 terminal type 3-48
3.1.36 user-interface 3-50
3.1.37 user-interface class 3-52
3.1.38 user-role 3-54
3.1.39 web idle-timeout 3-55

3章 ログイン

3.1 ログイン設定

いくつかのログインコマンドは user line view と user line class view の両方で有効です。

- user line view の設定は、user line にのみ適用されます。user line class view はクラスのすべての user line に適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。

3.1.1 authentication-mode

Syntax

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

undo authentication-mode

デフォルト

コンソールユーザの認証モードは password です。

VTY line の認証モードは password です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

none: 認証を無効にします。

password: ローカルパスワード認証を行います。

scheme: AAA 認証を行います。AAA の詳細はオペレーションマニュアル セクション 12 *ユーザアクセスと認証 "AAA"*を参照してください。

説明

authentication-mode コマンドは user line の認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

認証モードが **none** である場合、すべてのユーザは認証なしでログインすることができます。装置のセキュリティを改善するため、認証モードを **password** あるいは **scheme** にしてください。

VTY line view で、**authentication-mode** コマンドは **protocol inbound** コマンドと関連します。VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

認証モードを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

user line VTY 0 で認証モードを none にします。

<AP> system-view

[AP] line vty 0

[AP-line-vty0] authentication-mode none

user line VTY 0 で認証モードを password に設定し、パスワードを 321 に設定します。

<AP> system-view

[AP] line vty 0

[AP-line-vty0] authentication-mode password

[AP-line-vty0] set authentication password simple 321

user line VTY 0 で認証モードを scheme に設定します。ローカルユーザ 123 を設定し、パスワードを 321 に設定します。Telnet サービスを割り当て、ユーザのユーザロールを network-admin に割り当てます。

<AP> system-view

[AP] line vty 0

[AP-line-vty0] authentication-mode scheme

[AP-line-vty0] quit

[AP] local-user 123

[AP-luser-manage-123] password simple 321

[AP-luser-manage-123] service-type telnet

[AP-luser-manage-123] authorization-attribute user-role network-admin

関連コマンド

set authentication password

3.1.2 auto-execute command

注意:

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

Syntax

auto-execute command *command*

undo auto-execute command

デフォルト

無効

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

command: 自動で実行されるコマンドを指定します。

説明

auto-execute コマンドは console line view と console line class view ではサポートされません。

auto-execute コマンドを使用して変更された設定は、現在のセッションには適用されません。

ユーザが現在の user line にログインしたとき、装置は指定されたコマンドを自動で実行します。指定したコマンドが別の作業を引き起こす場合、装置は作業が完了するまでユーザの接続を切断しません。コマンドが他の作業を引き起こさない場合、装置はコマンド実行後にユーザの接続を切断します。

auto-execute command telnet *X.X.X.X* コマンドを設定すると、装置は Telnet ユーザを X.X.X.X のホストにリダイレクトさせます。ユーザが X.X.X.X との Telnet 接続を削除した場合、装置との接続は切断されます。

例

ユーザが VTY line 0 にログインした後、自動的に Telnet192.168.1.41 を実行するように設定します。

<AP> system-view

[AP] line vty 0

[AP-line-vty0] auto-execute command telnet 192.168.1.41

```
This action will lead to configuration failure through line-vty0. Are you sure?
[Y/N]:y
```

[AP-line-vty0]

設定を確認するため、192.168.1.40 に Telnet します。

装置は自動的に 192.168.1.41 に Telnet し、以下の出力が表示されます。

C:¥> telnet 192.168.1.40

```
<AP>
Trying 192.168.1.41 ...
Press CTRL+K to abort
Connected to 192.168.1.41 ...
<AP.41>
```

この動作は、Telnet で 192.168.1.41 に直接ログインすることと同一です。192.168.1.41 への Telnet 接続を終了するとき、同時に 192.168.1.40 への Telnet 接続も終了されます。

3.1.3 display ip http

Syntax

display ip http

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip http コマンドは HTTP サービスの設定とステータス情報を表示します。

例

HTTP サービスの設定とステータス情報を表示します。

<AP> display ip http

```
HTTP port: 80
ACL: 2222(basic)
Operation status: Enabled
```

表 3-1 コマンド出力

フィールド	説明
HTTP port	HTTPサービスのポート番号です。
ACL	HTTPアクセスを制御するために使用されるACLの数とタイプです。ACLを使用しない場合、このフィールドには **0** が表示されます。
Operation status	HTTPサービスが有効かどうかを示します。

関連コマンド

- **ip http acl**
- **ip http enable**
- **ip http port**

3.1.4 display ip https

Syntax

display ip https

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip https コマンドは HTTPS サービスの設定とステータス情報を表示します。

例

HTTPS サービスの設定とステータス情報を表示します。

<AP> display ip https

```
HTTPS port: 443
SSL server policy: test
Certificate access-control-policy: Not configured
ACL: 2222(advanced)
Operation status: Enabled
```

表 3-2 コマンド出力

フィールド	説明
HTTPS port	HTTPSサービスのポート番号です。
SSL server policy	HTTPSサービスに割り当てられたSSLサービスポリシーです。HTTPSサービスにSSLサービスポリシーが割り当てられていない場合、**Not configured**と表示されます。
Certificate access-control-policy	クライアントアクセス権の制御に使用される証明書属性ベースのアクセスコントロールポリシーです。HTTPSサービスにアクセスコントロールポリシーが割り当てられていない場合、**Not configured**と表示されます。
ACL	HTTPアクセスを制御するために使用されるACLの数とタイプです。ACLを使用しない場合、このフィールドには **0** が表示されます。
Operation status	HTTPサービスが有効かどうかを示します。

関連コマンド

- **ip https acl**
- **ip https enable**
- **ip https port**

3.1.5 display line

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

number1: user line の通し番号を指定します。設定範囲は 0～64 です。

console: console line を指定します。

vty: VTY line を指定します。

number2: user line のタイプごとの番号を指定します。設定範囲は 0～63 です。

summary: user line についての概要情報を表示します。このキーワードを指定しない場合、詳細な情報が表示されます。

説明

display line コマンドは user line の情報を表示します。

例

user line の情報を表示します。

<AP> display line 0

```
  Idx  Type     Tx/Rx      Modem Auth  Int       Location
+ 0    CON 0    9600       -     N     -         1/0

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

表 3-3 コマンド出力

フィールド	説明
Modem	モデムのモードがin/outを示します。デフォルトでは設定されていません。ハイフン(－)が表示されます。
Int	lineの物理ポートです。lineに物理ポートがない、あるいはコンソールlineの場合、ハイフン(－)が表示されます。
Location	lineの物理的な位置です。スロット番号/CPU番号の形式です。

すべての user line の概要情報を表示します。

<AP> display line summary

```
Line type : [CON]
        0:X
Line type : [VTY]
        1:UXXX XXXX XXXX XXXX
       17:XXXX XXXX XXXX XXXX
       33:XXXX XXXX XXXX XXXX
       49:XXXX XXXX XXXX XXXX
 1 lines used.     (U)
64 lines not used.  (X)
```

表 3-4 コマンド出力

フィールド	説明
number:status	*number*はuser line classの最初のuser lineの通し番号を示します。0からの番号です。*status*はuser line classのuser lineが使用されているかどうかを示します。Xは未使用でUは使用されています。 例えば、"2:UXXX X"が表示された場合、user line classには絶対番号2～6を使用する5つのuser lineが存在します。user line2は使用中で、その他のuser lineは未使用です。

3.1.6 display user-interface

Syntax

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

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

number1: user line の通し番号を指定します。設定範囲は 0～64 です。

console: console line を指定します。

vty: VTY line を指定します。

number2: user line のタイプごとの番号を指定します。設定範囲は 0～63 です。

summary: user line の概要を表示します。指定しない場合、詳細な情報を表示します。

説明

display user-interface コマンドは user line の情報を表示します。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**display line** コマンドと同一機能です。通常は **display line** コマンドを使用してください。

例

user line の情報を表示します。

<AP> display user-interface 0

```
  Idx  Type    Tx/Rx     Modem Auth  Int       Location
+ 0    CON 0   9600      -    N    -         1/0

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

表 3-5 コマンド出力

フィールド	説明
Modem	モデムのモードがin/outを示します。デフォルトでは設定されていません。ハイフン(－)が表示されます。
Int	lineの物理ポートです。lineに物理ポートがない、あるいはコンソールlineの場合、ハイフン(－)が表示されます。
Location	lineの物理的な位置です。スロット番号/CPU番号の形式です。

すべての user line の概要情報を表示します。

<AP> display user-interface summary

```
Line type : [CON]
        0:U
Line type : [VTY]
        2:UXXX X
 2 lines used.     (U)
 5 lines not used.  (X)
```

表 3-6 コマンド出力

フィールド	説明
number:status	*number*はuser line classの最初のuser lineの通し番号を示します。0からの番号です。*status*はuser line classのuser lineが使用されているかどうかを示します。Xは未使用でUは使用されています。 例えば、"2:UXXX X"が表示された場合、user line classには絶対番号2～6を使用する5つのuser lineが存在します。user line2は使用中で、その他のuser lineは未使用です。

3.1.7 display users

Syntax

display users [**all**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: 装置でサポートされるすべての user line を表示します。

説明

display users コマンドはオンライン CLI ユーザの情報を表示します。

例

オンライン CLI ユーザの情報を表示します。

< AP> display users

```
  Idx  Line     Idle      Time            Pid     Type
  10   VTY 0    00:10:49   Jun 11 11:27:32   320     TEL
+ 11   VTY 1    00:00:00   Jun 11 11:39:40   334     TEL

Following are more details.
VTY 0   :
       Location: 192.168.1.12
VTY 1   :
       Location: 192.168.1.26
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

出力は、2 つのユーザが装置にログインしたことを示します。一方は user line VTY 0 を使用し、もう一方（使用者自身）は VTY 1 を使用します。使用者の IP アドレスは 192.168.1.26 です。

表 3-7 コマンド出力

フィールド	説明
Idx	user lineの通し番号です。
Line	user lineのタイプとタイプごとの番号です。

フィールド	説明
Idle	ユーザがログインしてからの経過時間です。hh:mm:ssで表示します。
Time	ユーザのログイン時間です。
Pid	ユーザセッションのプロセスIDです。
Type	ユーザタイプです。 ● **TEL**—Telnetユーザです。 ● **SSH**—SSHユーザです。
+	カレントユーザが使用しているuser lineを示します。
Location	カレントユーザのIPアドレスです。

3.1.8 display web menu

Syntax

display web menu

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display web menu コマンドは、Web インタフェースのナビゲーション ツリー情報を表示します。このコマンドは、Web インタフェースのナビゲーション ツリーにすべてのオプションを表示します。

例

Web インタフェースのナビゲーション ツリー情報を表示します。

<AP> display web menu

.

3.1.9 display web users

Syntax

display web users

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display web users コマンドはオンライン Web ユーザを表示します。

例

オンライン Web ユーザを表示します。

<AP> display web users

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

表 3-8 コマンド出力

フィールド	説明
UserID	オンラインWebユーザを一意に識別するために使用されるIDです。
JobCount	ユーザによって接続が確立された数です。

3.1.10 escape-key

Syntax

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

undo escape-key

デフォルト

Ctrl+C

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

key-string: ショートカットキーを指定します。文字列あるいは ASCII コードで指定します。文字列は大文字、小文字を区別します（d と D を除く）。ASCII コードの設定範囲は 0～127 です。たとえば、**escape-key** 1 コマンドを設定した場合、ショートカットキーは Ctrl+A です。escape-key a コマンドを設定した場合、ショートカットキーは a です。Ctrl キーを使用する ASCII コードの詳細は表 3-9 を参照してください。

表 3-9 Ctrl キーを使用する ASCII コード

フィールド	説明
Ctrl+A	1
Ctrl+B	2
Ctrl+C	3
Ctrl+D	4
Ctrl+E	5
Ctrl+F	6
Ctrl+G	7
Ctrl+H	8
Ctrl+I	9

フィールド	説明
Ctrl+J	10
Ctrl+K	11
Ctrl+L	12
Ctrl+M	13
Ctrl+N	14
Ctrl+O	15
Ctrl+P	16
Ctrl+Q	17
Ctrl+R	18
Ctrl+S	19
Ctrl+T	20
Ctrl+U	21
Ctrl+V	22
Ctrl+W	23
Ctrl+X	24
Ctrl+Y	25
Ctrl+Z	26

default: エスケープキーを Ctrl+C に戻します。

説明

escape-key コマンドはエスケープキーを設定します。

undo escape-key コマンドはエスケープキーを無効にします。

実行したコマンドを中断する場合、エスケープキーを押下します。たとえば、**ping** コマンド、**tracert** コマンドを中断する場合に使用します。デフォルトで Ctrl+C が指定されているかどうかはコマンドの実装によって異なります。詳細はコマンドのガイドラインに従ってください。

エスケープキーとしてキーシーケンスを使用します。エスケープシーケンスとして 1 文字を指定する場合、実行したコマンドを中断するとき、キーを押下します。コマンドが実行されない場合、結果は以下の状況によります。

- ローカル装置を管理する場合、キーを押すと同一の文字列で入力されます。
- 別の装置に Telnet しリモート装置を管理する場合、キーを押しても動作しません。

undo escape-key コマンドは現在のエスケープキーを無効にします。

user line view で設定した場合、現在のセッションにすぐに適用します。user line class view で設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

現在のエスケープキーを表示する場合、**display current-configuration | include escape-key** コマンドを使用します。

例

console line 0 でエスケープキーとして a を設定します。

<AP> system-view

[AP] line console 0

[AP-line-console0] escape-key a

設定を確認します。

1) IP アドレス 192.168.1.49 に ping を実行します。-c パラメータを使用して ICMP エコーリクエストパケットの数を 20 に設定します。

<AP> ping -c 20 192.168.1.49

```
PING 192.168.1.49: 56  data bytes, press a to break
  Reply from 192.168.1.49: bytes=56 Sequence=1 ttl=255 time=3 ms
  Reply from 192.168.1.49: bytes=56 Sequence=2 ttl=255 time=3 ms
```

2) a を押下します。

システムはコマンドを中断し、user view に戻ります。

```
--- 192.168.1.49 ping statistics ---
  2 packet(s) transmitted
  2 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/3/3 ms
```

<AP>

3.1.11 free line

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

number1: user line の通し番号を指定します。設定範囲は 0～64 です。

console: console line を指定します。

vty: VTY line を指定します。

number2: user line のタイプごとの番号を指定します。設定範囲は 0～63 です。

説明

free line コマンドは user line を切断します。

カレントユーザを切断することはできません。

例

オンラインユーザを表示します。

<AP> display users

```
  Idx  Line     Idle      Time             Pid     Type
  10   VTY 0    00:10:49   Jun 11 11:27:32   320     TEL
+ 11   VTY 1    00:00:00   Jun 11 11:39:40   334     TEL

Following are more details.
VTY 0   :
       Location: 192.168.1.12
VTY 1   :
       Location: 192.168.1.26
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

user line VTY 1 を切断します。

<AP> free line vty 1

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

3.1.12 free user-interface

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

number1: user line の通し番号を指定します。設定範囲は 0～64 です。

console: console line を指定します。

vty: VTY line を指定します。

number2: user line のタイプごとの番号を指定します。設定範囲は 0～63 です。

説明

free user-interface コマンドは user line を切断します。

カレントユーザを切断することはできません。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**free line** コマンドと同一機能です。通常は **free line** コマンドを使用してください。

例

オンラインユーザを表示します。

<AP> display users

```
  Idx  LINE     Idle      Time             Pid     Type
  10   VTY 0    00:10:49   Jun 11 11:27:32   320     TEL
+ 11   VTY 1    00:00:00   Jun 11 11:39:40   334     TEL
Following are more details.
VTY 0   :
       Location: 192.168.1.12
VTY 1   :
       Location: 192.168.1.26
 +    : Current operation user.
 F    : Current operation user works in async mode.
```

VTY 1 を切断します。

<AP> free user-interface vty 1

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

3.1.13 free web users

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての Web ユーザを指定します。

user-id *user-id*: Web ユーザの ID を指定します。15 桁の 16 進数表示です。ユーザを識別するため、各 Web ユーザに一意の ID を割り当てます。

user-name: Web ユーザのユーザ名を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

free web users コマンドはオンライン Web ユーザをログオフします。

例

すべてのオンライン Web ユーザをログオフします。

<AP> free web users all

関連コマンド

display web users

3.1.14 history-command max-size

Syntax

history-command max-size *size-value*

undo history-command max-size

デフォルト

10

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

size-value: 履歴コマンドをバッファに保存できる最大数を指定します。設定範囲は 0～256 です。

説明

history-command max-size コマンドは user line のコマンドの履歴をバッファに保存する最大数を設定します。

undo history-command max-size コマンドはデフォルトに戻します。

各 user line は、実行された有効なコマンドを別のバッファに保存します。バッファサイズはバッファにいくつの履歴コマンドを保存できるかを決定します。

カレント user line で保存された履歴コマンドを表示する場合、矢印キーの↑あるいは↓を押下するか、**display history-command** コマンドを実行します。詳細はオペレーションマニュアルのセクション 1 *基本機能　“CLI の概要”* を参照してください。

CLI セッションを終了すると、履歴コマンドのバッファはクリアされます。

user line view での設定は現在のセッションにすぐさま適用されます。user line class view での設定は、設定が行われた後、ログインセッションで適用されます。

例

user line Console 0 のコマンドの履歴をバッファに記録する最大数を 20 に設定します。

<AP> system-view

[AP] line console 0

[AP-line-console0] history-command max-size 20

3.1.15 idle-timeout

Syntax

idle-timeout *minutes* [*seconds*]

undo idle-timeout

デフォルト

10 分

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

minutes: タイムアウト時間の分を指定します。設定範囲は 0～35791 です。デフォルトは 10 分です。

seconds: タイムアウト時間の秒を指定します。設定範囲は 0～59 です。デフォルトは 0 秒です。

説明

idle-timeout コマンドは CLI セッションがタイムアウトする時間を設定します。

undo idle-timeout コマンドはデフォルトに戻します。

ユーザ操作が実行されずにタイムアウト時間が経過すると、ユーザ接続を切断します。

タイムアウト時間を 0 にすると、**idle-timeout** コマンドを無効にし、セッションがタイムアウトしません。

user line view での設定は現在のセッションにすぐさま適用されます。user line class view での設定は、設定が行われた後、ログインセッションで適用されます。

例

user line Console 0 の CLI セッションのタイムアウト時間を 1 分 30 秒に設定します。

<AP> system-view

[AP] line console 0

[AP-line-console0] idle-timeout 1 30

3.1.16 ip http acl

Syntax

ip http acl [advanced] { *acl-number* | **name** *acl-name* }

ip http acl mac { *acl-number* | **name** *acl-name* }

undo ip http acl

undo ip http acl mac

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

advanced: 拡張 ACL を指定します。

mac: レイヤ 2 ACL を指定します。

acl-number: ACL の番号を次のいずれかの範囲で指定します。

- 基本 ACL の場合は 2000～2999
- 拡張 ACL の場合は 3000～3999
- レイヤ 2 ACL の場合は 4000～4999

name *acl-name*: ACL の名前を指定します。大文字と小文字を区別しません。1～63 文字です。英文字ではじめてください。混乱を防ぐため **all** には設定できません。指定された ACL は、ACL が存在する場合にのみ適用されます。

説明

ip http acl コマンドは HTTP サービスに ACL を適用します。

undo ip http acl コマンドはデフォルトに戻します。

advanced キーワードまたは **mac** キーワードを指定しない場合は、IPv4 基本 ACL を指定します。

HTTP サービスに適用される拡張 ACL では、次の一致基準のみが有効になります。

- 送信元および宛先 IP アドレス
- 送信元ポートと宛先ポート
- トランスポート層プロトコル

HTTP サービスに適用されるレイヤ 2 ACL では、送信元 MAC アドレスの一致基準だけが有効になります。

適用された ACL に許可されたクライアントのみ、HTTP で装置にアクセスできます。

指定した ACL が存在しないか、または有効なルールがない場合、すべてのユーザは HTTP で装置にアクセスできます。

ip http acl コマンドを複数回実行する場合、最新の設定が適用されます。

例

10.10.0.0/16 のユーザのみが HTTP を通して装置にアクセスできるように HTTP サービスに ACL2001 を割り当てます。

<AP> system-view

[AP] acl basic 2001

[AP-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255

[AP-acl-ipv4-basic-2001] quit

[AP] ip http acl 2001

関連コマンド

acl（コマンドマニュアルのセクション 13 セキュリティ" *ACL* " ）

3.1.17 ip http enable

Syntax

ip http enable

undo ip http enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip http enable コマンドは HTTP サービスを有効にします。

undo ip http enable コマンドは HTTP サービスを無効にします。

ユーザが HTTP を通して装置にアクセスする場合、HTTP サービスを有効にする必要があります。

Web ログインリクエストには、ユーザ名とパスワードが含まれます。セキュリティの観点から、装置は Web ログインリクエストの転送には常に HTTPS を使用します。HTTP ログインを設定するために、HTTPS サービスも有効にする必要があります。

例

HTTP サービスを有効にします。

<AP> system-view

[AP] ip http enable

関連コマンド

ip https enable

3.1.18 ip http port

Syntax

ip http port *port-number*

undo ip http port

デフォルト

80

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: HTTP サービスのポート番号を指定します。設定範囲は 1～65535 です。

説明

ip http port コマンドは HTTP サービスのポート番号を指定します。

undo ip http port コマンドはデフォルトに戻します。

HTTP サービスが有効であるとき、HTTP サービスのポート番号を変更した場合、HTTP サービスを再度有効にし、すべての HTTP 接続を切断します。再度ログインする場合、ユーザは Web ブラウザのアドレスバーで新しい URL を入力する必要があります。

例

HTTP サービスのポート番号を 80 に指定します。

<AP> system-view

[AP] ip http port 80

3.1.19 ip https acl

Syntax

ip https acl [advanced] { *acl-number* | **name** *acl-name* }

ip https acl mac { *acl-number* | **name** *acl-name* }

undo ip https acl

undo ip https acl mac

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

advanced: 拡張 ACL を指定します。

mac: レイヤ 2 ACL を指定します。

acl-number: ACL の番号を次のいずれかの範囲で指定します。

- 基本 ACL の場合は 2000～2999
- 拡張 ACL の場合は 3000～3999
- レイヤ 2 ACL の場合は 4000～4999

name *acl-name*: ACL の名前を指定します。大文字と小文字を区別しません。1～63 文字です。英文字ではじめてください。混乱を防ぐため **all** には設定できません。指定された ACL は、ACL が存在する場合にのみ適用されます。

説明

ip https acl コマンドは HTTPS サービスに ACL を割り当てます。

undo ip https acl コマンドは ACL の割り当てを削除します。

advanced キーワードまたは **mac** キーワードを指定しない場合は、IPv4 基本 ACL を指定します。

HTTP サービスに適用される拡張 ACL では、次の一致基準のみが有効になります。

- 送信元および宛先 IP アドレス
- 送信元ポートと宛先ポート
- トランスポート層プロトコル

HTTP サービスに適用されるレイヤ 2 ACL では、送信元 MAC アドレスの一致基準だけが有効になります。

適用された ACL に許可されたクライアントのみ、HTTPS で装置にアクセスできます。

指定した ACL が存在しないか、または有効なルールがない場合、すべてのユーザは HTTPS で装置にアクセスできます。

HTTPS サービスに適用された ACL は HTTPS と HTTP ログインの両方を制御します。装置にアクセスするため、HTTP クライアントは以下の ACL によって許可する必要があります。

- HTTP サービスに適用する ACL
- HTTPS サービスに適用する ACL

ip https acl コマンドを複数実行した場合、最後に行った設定が適用されます。

例

10.10.0.0/16 のユーザのみが HTTP あるいは HTTPS を通して装置にアクセスできるように ACL2001 を割り当てます。

<AP> system-view

[AP] acl basic 2001

[AP-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255

[AP-acl-ipv4-basic-2001] quit

[AP] ip https acl 2001

関連コマンド

acl（コマンドマニュアルのセクション 8 *ACL and QoS* ）

3.1.20 ip https enable

Syntax

ip https enable

undo ip https enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip https enable コマンドは HTTPS サービスを有効にします。

undo ip https enable コマンドは HTTPS サービスを無効にします。

ユーザが HTTPS を通して装置にアクセスする場合、HTTPS サービスを有効にする必要があります。

HTTPS サービスを有効にすると、SSH ハンドシェークのネゴシエーションプロセスが開始します。

- 装置がローカル証明書を持っている場合、SSH ハンドシェークのネゴシエーションは成功し、HTTPS サービスを開始します。
- 装置がローカル証明書を持っていない場合、証明書アプリケーションプロセスが開始します。証明書アプリケーションプロセスは長い時間がかかるため、SSH ハンドシェークは失敗し、HTTPS サービスが開始されない可能性があります。この問題を解決するため、HTTPS サービスが有効になるまで **ip https enable** コマンドを再度実行します。

例

HTTPS サービスを有効にします。

<AP> system-view

[AP] ip https enable

3.1.21 ip https port

Syntax

ip https port *port-number*

undo ip https port

デフォルト

443

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: HTTPS サービスのポート番号を指定します。設定範囲は 1～65535 です。

説明

ip https port コマンドは HTTPS サービスのポート番号を指定します。

undo ip https port コマンドはデフォルトに戻します。

HTTPS サービスが有効であるとき、HTTPS サービスのポート番号を変更した場合、HTTPS サービスを再度有効にし、すべての HTTPS 接続を切断します。再度ログインする場合、ユーザは Web ブラウザのアドレスバーで新しい URL を入力する必要があります。

例

HTTPS サービスのポート番号を 8080 に指定します。

<AP> system-view

[AP] ip https port 8080

3.1.22 line

Syntax

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

View

System view

定義済みユーザロール

network-admin

パラメータ

first-number1: 最初の user line の通し番号を指定します。設定範囲は 0～64 です。

last-number1: 最後の user line の通し番号を指定します。*first-number1* より大きくなければなりません。

console: console line を指定します。

vty: VTY line を指定します。

first-number2: 最初の user line のタイプごとの番号を指定します。設定範囲は 0～63 です。

last-number2: 最後の user line のタイプごとの番号を指定します。*first-number2* より大きくなければなりません。

説明

line コマンドは 1 つ以上の user line view に移行します。

シングル user line に設定を行うために、このコマンドを使用して user line view に移行します。

同じ設定を複数の user line に行うために、このコマンドを使用して複数の user line view に移行します。

例

user line Console 0 の view に移行します。

<AP> system-view

[AP] line console 0

[AP-line-console0]

user lines VTY 0～VTY 4 の view に移行します。

<AP> system-view

[AP] line vty 0 4

[AP-line-vty0-4]

関連コマンド

line class

3.1.23 line class

Syntax

line class { **console** | **vty** }

View

System view

定義済みユーザロール

network-admin

パラメータ

console: console line class view を指定します。

vty: VTY line class view を指定します。

説明

line class コマンドは user line class view に移行します。

line class のすべての user line で設定を同一にするために、user line class view に移行します。

user line class view では以下のコマンドを実行することができます。

- **auto-execute command**
- **authentication-mode**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

いくつかのログインコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定は user line で適用されます。user line class view の設定は class のすべての user line で適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。
- user line view の設定はすぐに適用され、オンラインユーザに影響します。user line class view の設定は設定が完了したのちにログインしたユーザのみ適用されます。user line class view の設定はオンラインユーザに影響しません。

例

VTY line class view でユーザ接続タイムアウト時間を 15 分に設定します。

<AP> system-view

[AP] line class vty

[AP-line-class-vty] idle-timeout 15

関連コマンド

line

3.1.24 lock

Syntax

lock

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

説明

lock コマンドは現在の user line をロックします。

許可されていないユーザが user line で操作を使用しないように防止します。

lock コマンドを実行した後、ロックされていない user line のパスワードを入力し、再度パスワードを入力します。

user line を解除する場合、Enter キーを押下し、正しいパスワードを入力します。

例

現在の user line をロックします。その後ロックを解除します。

<AP> lock

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


                locked !
// The user line is locked. To unlock it, press Enter and enter the password:
Password:
```

<AP>

3.1.25 protocol inbound

Syntax

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

undo protocol inbound

デフォルト

all

View

VTY line view

VTY line class view

定義済みユーザロール

network-admin

パラメータ

all: SSH、Telnet のプロトコルをサポートします。

ssh: SSH のプロトコルをサポートします。

telnet: Telnet のプロトコルをサポートします。

説明

protocol inbound コマンドはサポートするプロトコルを設定します。

undo protocol inbound コマンドはデフォルトに戻します。

SSH をサポートするため user line を設定する前に、**authentication-mode** コマンドを使用して user line の認証モードを scheme に設定してください。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

user line view で設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

VTY line view で、protocol inbound コマンドは **authentication-mode** コマンドと関連します。VTY line view で 2 つのコマンドのうち、1 つコマンドのみデフォルトでない認証モードである場合、もう一方のコマンドは VTY line class view の設定に関わらず、デフォルトの認証モードを使用します。

例

user line VTY 0～4 で SSH のみを有効にするように設定します。

<AP> system-view

[AP] line vty 0 4

[AP-line-vty0-4] authentication-mode scheme

[AP-line-vty0-4] protocol inbound ssh

SSH を有効にし、VTY line class view で認証モードを scheme に設定します。user line VTY 0～VTY 4 ですべてのプロトコルを有効にし、user line で認証を無効にします。

<AP> system-view

[AP] line class vty

[AP-line-class-vty] authentication-mode scheme

[AP-line-class-vty] protocol inbound ssh

[AP-line-class-vty] line vty 0 4

[AP-line-vty0-4] authentication-mode none

設定を確認します。

1) 装置に Telnet します。

<Client> telnet 192.168.1.241

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

<Server>

認証なしでログインしました。

2) オンライン CLI ユーザの情報を表示します。

<Server> display users

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

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

出力は、ユーザは VTY 0 を使用していることを示します。user line view の設定は適用されています。

3.1.26 screen-length

Syntax

screen-length *screen-length*

undo screen-length

デフォルト

24 行

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

screen-length: 画面上で一度に表示される行の最大数を指定します。設定範囲は 0～512 です。0 に設定した場合、出力画面のスクロールは停止しません。

説明

screen-length コマンドは画面上で一度に表示される行の最大数を設定します。

undo screen-length コマンドはデフォルトに戻します。

出力画面に表示される実際の行数は端末のモニタの仕様によって制限されます。

たとえば、画面上で一度に表示される行の最大数を 40 に設定した場合、装置はすぐに端末に 40 行を送信します。もし端末のモニタの仕様が 24 である場合、出力画面には最後の 24 行のみが表示されます。前の 16 行を表示する場合、**PgUp** キーを押下します。

停止したのち、出力を継続する場合、スペースキーを押下します。出力画面のスクロールの停止機能はデフォルトで有効です。

設定を変更した場合、すぐに現在のセッションに適用します。user line class view での設定は、設定が行われた後、ログインセッションで適用されます。

例

user line Console 0 で一度に表示される行の最大数を 30 行に設定します。

<AP> system-view

[AP] line console 0

[AP-line- console 0] screen-length 30

関連コマンド

screen-length disable

3.1.27 send

Syntax

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

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての user line を指定します。

number1: user line の通し番号を指定します。設定範囲は 0～64 です。

console: console line を指定します。

vty: VTY line を指定します。

number2: user line のタイプごとの番号を指定します。設定範囲は 0～63 です。

説明

send コマンドはオンラインログインユーザにメッセージを送信します。

メッセージを終了する場合、**Enter** キーを押下します。メッセージをキャンセルし、user view に戻る場合、**Ctrl+C** キーを押下します。

ほかのオンラインユーザに影響を及ぼす操作を実行する前に、オンラインユーザに通知するために使用することができます。たとえば装置を再起動する場合などに使用します。

例

VTY 1 の user に通知するため、メッセージを送信します。

<AP> send vty 1

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

メッセージは以下の例のようにユーザの設定端末の画面に表示されます。

[AP]

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

3.1.28 set authentication password

Syntax

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

undo set authentication password

デフォルト

コンソールユーザのパスワード設定は qx_admin です。

line class vty は qx_admin です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

hash: 暗号テキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。

password: 大文字、小文字が区別されたパスワードを指定します。**simple** が指定された場合、設定範囲は 1～16 文字です。**hash** が指定された場合、設定範囲は 1～110 文字です。

説明

set authentication password コマンドはパスワード認証のパスワードを設定します。

undo set authentication password コマンドはパスワードを削除します。

セキュリティのため、保存されたパスワードは設定に関わらず常に暗号テキストで表示されます。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

パスワードを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

user line Console 0 でパスワード認証のパスワード hello を設定します。

<AP> system-view

[AP] line console 0

[AP-line-console0] authentication-mode password

[AP-line-console0] set authentication password simple hello

関連コマンド

authentication-mode

3.1.29 shell

Syntax

shell

undo shell

デフォルト

有効

View

User line view

User line class view

定義済みユーザロール

network-admin

説明

shell コマンドは user line の端末サービスを有効にします。

undo shell コマンドは user line の端末サービスを無効にします。

console line view あるいは console line class view でコマンドは **undo shell** サポートしていません。

現在使用している user line の端末サービスを無効にすることはできません。

装置が Telnet あるいは SSH サーバとして動作するとき、**undo shell** コマンドを設定することはできません。

user line class view で **undo shell** コマンドが設定された場合、class の user line の view で **shell** コマンドを設定することはできません。

端末サービスが有効であるとき、user line は装置へのログインに使用されます。装置がリダイレクトサーバとして稼働している場合、user line はリダイレクトサービスに使用されます。user line は 1 回につき、1 つの処理のみ行うことができます。

例

user line からユーザが装置にログインできないようにするため、VTY line 0～VTY line 4 の端末サービスを無効にします。

<AP> system-view

[AP] line vty 0 4

[AP-line-vty0-4] undo shell

```
Disable ui-vty0-4 , are you sure? [Y/N]:y
```

[AP-line-vty0-4]

3.1.30 telnet server acl

Syntax

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

undo telnet server acl

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

mac: レイヤ 2 の ACL を指定します。異なるタイプの ACL を指定する場合は、このキーワードを指定しないでください。

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

説明

telnet server acl コマンドは Telnet ログインのフィルタリングを有効にします。

undo telnet server acl コマンドはデフォルトに戻します。

ACL が Telnet サービスに適用されない場合、すべてのユーザが装置に Telnet 接続できます。Telnet ログインを制御するには、ACL によって許可されたユーザのみが装置に Telnet 接続できるように、存在しルールを持つ ACL を指定します。存在しない ACL またはルールを持たない ACL を指定した場合、どのユーザも装置に Telnet 接続できません。

ACL の詳細は、コマンドマニュアルのセクション 13 *セキュリティ "ACL"*を参照してください。

このコマンドを複数回実行すると、最新の設定が有効になります。

このコマンドは、既存の Telnet 接続には有効になりません。

例

1.1.1.1 のユーザのみに装置への Telnet 接続を許可します。

<AP> system-view

[AP] acl basic 2001

[AP-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0

[Ap-acl-ipv4-basic-2001] quit

[AP] telnet server acl 2001

3.1.31 telnet server acl-deny-log enable

Syntax

telnet server acl-deny-log enable

undo telnet server acl-deny-log enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

telnet server acl-deny-log enable コマンドは Telnet ログイン制御 ACL によって拒否された Telnet ログイン試行のログを有効にします。

undo telnet server acl-deny-log enable コマンドは Telnet ログイン制御 ACL によって拒否された Telnet ログイン試行のログを無効にします。

Telnet ログイン制御 ACL によって許可されたクライアントだけが、Telnet で装置に接続できます。このログ機能は、Telnet ログイン制御 ACL によって拒否された Telnet ログイン試行のログメッセージを生成します。

ログメッセージの出力については、オペレーションマニュアルのセクション 2 *システム管理　“Information Center”* を参照してください。

例

ログを有効にします。

<AP> system-view

[AP] telnet server acl-deny-log enable

関連コマンド

telnet server acl

3.1.32 telnet server dscp

Syntax

telnet server dscp *dscp-value*

undo telnet server dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP 値を指定します。設定範囲は 0～63 です。

説明

telnet server dscp コマンドは Telnet サーバで Telnet パケットを送信する IPv4 の DSCP 値を設定します。

undo telnet server dscp コマンドはデフォルトに戻します。

DSCP 値は IPv4 パケットの ToS フィールドで送信されます。パケットを転送する優先度を示します。

例

Telnet サーバで Telnet パケットを送信する IPv4 の DSCP 値を 30 に設定します。

<AP> system-view

[AP] telnet server dscp 30

3.1.33 telnet server enable

Syntax

telnet server enable

undo telnet server enable

デフォルト

Telnet サーバは、無効です。

View

System view

定義済みユーザロール

network-admin

説明

telnet server enable コマンドは Telnet サーバ機能を有効にします。

undo telnet server enable コマンドは Telnet サーバ機能を無効にします。

管理者は Telnet サーバ機能が有効であるときのみ装置に Telnet を行うことができます。

例

Telnet サーバ機能を有効にします。

<AP> system-view

[AP] telnet server enable

3.1.34 telnet server port

Syntax

telnet server port port-number

undo telnet server port

デフォルト

IPv4 Telnet サービスのポート番号は、23 です。.

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: ポート番号を指定します。

設定可能範囲は、23 または 1025 ～ 65535 です。

説明

telnet server port を使用して、IPv4 Telnet サービスのポート番号を指定します。

undo telnet server port を使用して、デフォルトを戻します。

このコマンドは、IPv4 Telnet サーバへの既存のすべての Telnet 接続を終了します。

Telnet サービスを使用するには、ユーザは Telnet 接続を再確立する必要があります。

例

IPv4 Telnet サービスのポート番号を 1025 に設定します。

<AP> system-view

[AP] telnet server port 1025

3.1.35 terminal type

Syntax

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

undo terminal type

デフォルト

ANSI

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

ansi: 端末の表示タイプを ANSI に指定します。

vt100: 端末の表示タイプを VT100 に指定します。

説明

terminal type コマンドは端末の表示タイプを指定します。

undo terminal type コマンドはデフォルトに戻します。

装置は端末の表示タイプ ANSI と VT100 をサポートします。NEC は装置と端末の両方で表示タイプを VT100 に設定することを推奨します。

装置あるいは端末のどちらかが ANSI を使用している場合、コマンドラインが 80 文字を越えたときにカーソル位置のエラーなどの表示に関する問題が発生する可能性があります。

このコマンドは user line view および user line class view の両方でサポートしています。user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。

端末の表示タイプを変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

例

端末の表示タイプを VT100 に設定します。

<AP> system-view

[AP] line vty 0

[AP-line-vty0] terminal type vt100

3.1.36 user-interface

Syntax

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

View

System view

定義済みユーザロール

network-admin

パラメータ

first-number1: 最初の user line の通し番号を指定します。設定範囲は 0～64 です。

last-number1: 最後の user line の通し番号を指定します。*first-number1* より大きくなければなりません。

console: console line を指定します。

vty: VTY line を指定します。

first-number2: 最初の user line のタイプごとの番号を指定します。設定範囲は 0～63 です。

last-number2: 最後の user line のタイプごとの番号を指定します。*first-number2* より大きくなければなりません。

説明

user-interface コマンドは 1 つ以上の user line view に移行します。

1 つの user line を設定する場合、**user-interface** コマンドを使用して user line view に移行します。

複数の user line で同一の設定を行う場合、**user-interface** コマンドを使用して複数の user line view に移行します。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**line** コマンドと同一機能です。通常は **line** コマンドを使用してください。

例

user line Console 0 の view に移行します。

<AP> system-view

[AP] user-interface console 0

[AP-line-console0]

VTY 0～VTY 4 の view に移行します。

<AP> system-view

[AP] user-interface vty 0 4

[AP-line-vty0-4]

関連コマンド

user-interface class

3.1.37 user-interface class

Syntax

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

View

System view

定義済みユーザロール

network-admin

パラメータ

console: console line class view を指定します。

vty: VTY line class view を指定します。

説明

user-interface class コマンドは user line class view に移行します。

このコマンドは古いソフトウェアバージョンで使用していたユーザのためにサポートされているコマンドです。古いソフトウェアバージョンで動作するコマンドです。**line class** コマンドと同一機能です。通常は **line class** コマンドを使用してください。

line class のすべての user line で設定を同一にするために、user line class view に移行します。

user line class view では以下のコマンドを実行することができます。

- **auto-execute command**
- **authentication-mode**
- **history-command max-size**
- **idle-timeout**
- **protocol inbound**
- **screen-length**
- **set authentication password**
- **shell**
- **terminal type**
- **user-role**

いくつかのログインコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定は user line で適用されます。user line class view の設定は class のすべての user line で適用されます。
- user line view と user line class view のどちらかの view でデフォルトでない設定がある場合、デフォルトでない設定は、もう一方のデフォルト設定よりも優先されます。user line view のデフォルトでない設定は user line class view のデフォルトでない設定よりも優先されます。

- user line view の設定はすぐに適用され、オンラインユーザに影響します。user line class view の設定は設定が完了したのちにログインしたユーザのみ適用されます。user line class view の設定はオンラインユーザに影響しません。

例

VTY line class view でユーザ接続タイムアウト時間を 15 分に設定します。

<AP> system-view

[AP] user-interface class vty

[AP-line-class-vty] idle-timeout 15

関連コマンド

user-interface

3.1.38 user-role

Syntax

user-role *role-name*

undo user-role [*role-name*]

デフォルト

コンソールユーザのユーザロールは network-admin です。

VTY line のユーザロールは network-admin です。

View

User line view

User line class view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。大文字、小文字を区別します。範囲は 1～63 です。ユーザロールはユーザ定義あるいは定義済みのユーザロールがあります。定義済みは network-admin、network-operator、level-0～level-15 があります。**undo user-role** コマンドで *role-name* を指定しない場合、デフォルトのユーザロールに戻します。

説明

user-role コマンドは user line でログインしたユーザがユーザロールを取得できるように user line にユーザロールを割り当てます。

undo user-role コマンドはユーザロールを削除あるいはデフォルトに戻します。

network-admin あるいはレベル 15 のユーザロールが割り当てられたユーザのみコマンドを実行することができます。実行権限があったとしてもほかのユーザはコマンドを実行できません。

このコマンドは user line view および user line class view の両方でサポートしています。

- user line view の設定がデフォルトでないとき、user line view の設定が適用されます。
- user line view の設定がデフォルトで user line class view の設定がデフォルトでないとき、user line class view の設定が適用されます。

設定を変更した場合、現在のセッションに影響しません。次にログインしたときに適用されます。

user line に 64 のユーザロールを割り当てることができます。user line からログインしたユーザはすべてのユーザロールを取得します。

例

ユーザロール network-admin を VTY ライン 0～63 に割り当てます。

<AP> system-view

[AP] line vty 0 63

[AP-line-vty0-63] user-role network-admin

3.1.39 web idle-timeout

Syntax

web idle-timeout *idle-time*

undo web idle-timeout

デフォルト

10 分

View

System view

定義済みユーザロール

network-admin

パラメータ

idle-time: タイムアウトタイマーを指定します。設定範囲は 1～999 分です。

説明

web idle-timeout コマンドは Web ユーザの接続のタイムアウトタイマーを設定します。

undo web idle-timeout コマンドはデフォルトに戻します。

許可されていないアクセスを防ぐため、アイドルタイムアウト時間内にマウスあるいはキーボードの動作がない場合、システムは自動でユーザの接続を切断します。

このコマンドは現在の Web 接続に即座に適用されます。

例

Web ユーザの接続のタイムアウトタイマーを 100 分に設定します。

<AP> system-view

[AP] web idle-timeout 100

目次

このセクションのページは **1-x-x** です。

4 章 FTP と TFTP 4-1
4.1 FTP クライアント設定コマンド 4-1
4.1.1 ? 4-2
4.1.2 ascii 4-3
4.1.3 binary 4-4
4.1.4 bye 4-5
4.1.5 cd 4-6
4.1.6 cdup 4-8
4.1.7 close 4-9
4.1.8 debug 4-10
4.1.9 delete 4-11
4.1.10 dir 4-12
4.1.11 disconnect 4-14
4.1.12 display ftp client source 4-15
4.1.13 ftp 4-16
4.1.14 ftp client source 4-18
4.1.15 get 4-20
4.1.16 help 4-21
4.1.17 lcd 4-22
4.1.18 ls 4-23
4.1.19 mkdir 4-25
4.1.20 newer 4-26
4.1.21 open 4-27
4.1.22 passive 4-28
4.1.23 put 4-29
4.1.24 pwd 4-30
4.1.25 quit 4-31
4.1.26 rhelp 4-31
4.1.27 rmdir 4-34
4.1.28 user 4-34
4.1.29 verbose 4-35
4.2 TFTP クライアント設定コマンド 4-1
4.2.1 tftp 4-1
4.2.2 tftp client source 4-3
4.2.3 tftp-server acl 4-4

4章 FTP と TFTP

4.1 FTPクライアント設定コマンド

FTP クライアント設定コマンドを実行する前、FTP サーバでのユーザの許可設定が適用されていることを確認してください。許可設定は、作業ディレクトリ下のファイルの参照、ファイルの読み込み、ダウンロード、アップロード、ファイルのリネーム、ファイルの削除、ディレクトリの作成があります。

この章の FTP クライアントのコマンドは、装置によってサポートされていますが、正常に動作するかどうかは FTP サーバに依存します。

このセクションの例の出力例は FTP サーバの種類によって異なる場合があります。

4.1.1 ?

Syntax

? [*command-name*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

command-name: FTP クライアントでサポートされるコマンドを指定します。

説明

? コマンドは FTP クライアントでサポートされるすべてのコマンドを表示します。

? *command-name* コマンドはコマンドのヘルプ情報を表示します。

FTP client view において**?**コマンドは、**help** コマンドと同一です。

例

FTP クライアントでサポートされるすべてのコマンドを表示します。

ftp> ?

```
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

dir コマンドのヘルプ情報を表示します。

ftp> ? dir

```
dir             list contents of remote directory
```

関連コマンド

help

4.1.2 ascii

Syntax

ascii

デフォルト

バイナリモード

View

FTP client view

定義済みユーザロール

network-admin

説明

ascii コマンドはファイルの転送モードを ASCII モードに設定します。

- **バイナリモード**－非テキストファイル（プログラムファイルや絵）を転送します。
- **ASCII モード**－テキストファイルを転送します。

FTP サーバにログイン後のみコマンドを設定することができます。

装置が FTP サーバとして動作するとき、転送モードは FTP クライアントによって決定します。装置が FTP クライアントとして動作するとき、転送モードを設定することができます。

例

転送モードを ASCII モードに設定します。

ftp> ascii

```
200 TYPE is now ASCII
```

関連コマンド

binary

4.1.3 binary

Syntax

binary

デフォルト

バイナリモード

View

FTP client view

定義済みユーザロール

network-admin

説明

binary コマンドはファイルの転送モードをバイナリモードに設定します。このモードはフローモードと呼ばれます。

ascii コマンドはファイルの転送モードを ASCII モードに設定します。

- **バイナリモード**－非テキストファイル（プログラムファイルや絵）を転送します。
- **ASCII モード**－テキストファイルを転送します。

FTP サーバにログイン後のみコマンドを設定することができます。

装置が FTP サーバとして動作するとき、転送モードは FTP クライアントによって決定します。装置が FTP クライアントとして動作するとき、転送モードを設定することができます。

例

転送モードをバイナリモードに設定します。

ftp> binary

```
200 TYPE is now 8-bit binary
```

関連コマンド

ascii

4.1.4 bye

Syntax

bye

View

FTP client view

定義済みユーザロール

network-admin

説明

bye コマンドは FTP サーバの接続を終了し、user view に戻ります。

装置とリモート FTP サーバ間で接続が確立していない場合、user view に戻ります。

例

FTP サーバの接続を終了し、user view に戻ります。

ftp> bye

```
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
```

<AP>

関連コマンド

quit

4.1.5 cd

Syntax

cd { *directory* | **..** | */* }

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: [*drive*:][*/*]*path* の形式のターゲットディレクトリ名を指定します。ここでは記憶媒体の名前を示します。通常はフラッシュあるいは CF です。ターゲットディレクトリが存在しない場合、**cd** コマンドは現在の作業ディレクトリを変更しません。ドライブ情報がない場合、現在のディレクトリのフォルダあるいはサブフォルダを示します。*drive* と *path* の引数についての詳細はオペレーションマニュアルのセクション 1 *基本機能 "FTP と TFTP"* を参照してください。

..: 上位のディレクトリに戻ります。**cd ..**コマンドは **cdup** コマンドを実行するのと同一です。現在の作業ディレクトリが FTP ルートディレクトリである場合、**cd ..**はルートディレクトリに戻ります。

/: FTP ルートディレクトリに戻ります。

説明

cd コマンドは FTP サーバの現在の作業ディレクトリを別のディレクトリに変更します。

FTP サーバにログインした後のみ実行できます。

アクセスできるディレクトリは FTP サーバによって許可されている必要があります。

例

作業ディレクトリを現在のディレクトリのサブディレクトリ logfile に変更します。

ftp> cd logfile

```
250 OK. Current directory is /logfile
```

作業ディレクトリを FTP ルートディレクトリのサブディレクトリフォルダに変更します。

ftp> cd /folder

```
250 OK. Current directory is /folder
```

作業ディレクトリを現在のディレクトリの上位ディレクトリに変更します。

ftp> cd ..

```
250 OK. Current directory is /
```

作業ディレクトリを FTP ルートディレクトリに変更します。

ftp> cd /

```
250 OK. Current directory is /
```

関連コマンド

- **cdup**
- **pwd**

4.1.6 cdup

Syntax

cdup

View

FTP client view

定義済みユーザロール

network-admin

説明

cdup コマンドは FTP サーバの上位ディレクトリに移行します。

FTP サーバにログインした後のみ実行できます。

現在のディレクトリが FTP ルートディレクトリである場合、このコマンドは作業ディレクトリを変更しません。

例

作業ディレクトリを上位ディレクトリに移行します。

ftp> pwd

```
257 "/ftp/subdir" is your current location
```

ftp> cdup

```
250 OK. Current directory is /ftp
```

ftp> pwd

```
257 "/ftp" is your current location
```

関連コマンド

- **cd**
- **pwd**

4.1.7 close

Syntax

close

View

FTP client view

定義済みユーザロール

network-admin

説明

close コマンドは FTP client view から移動することなく、FTP サーバの接続を終了します。

FTP サーバにログインした後のみ実行できます。

例

FTP client view から移動することなく、FTP サーバの接続を終了します。

ftp> close

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

関連コマンド

disconnect

4.1.8 debug

Syntax

debug

デフォルト

無効

View

FTP client view

定義済みユーザロール

network-admin

説明

debug コマンドは FTP クライアントのデバッグを無効あるいは有効に設定します。

FTP クライアントのデバッグが有効であるとき、このコマンドを使用して FTP クライアントのデバッグを無効にします。

FTP クライアントのデバッグが無効であるとき、このコマンドを使用して FTP クライアントのデバッグを有効にします。

例

FTP クライアントのデバッグを有効にし、その後、無効にします。

ftp> debug

```
Debugging on (debug=1).
```

ftp> debug

```
Debugging off (debug=0).
```

4.1.9 delete

Syntax

delete *remotefile*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのファイル名を指定します。

説明

delete コマンドは FTP サーバのファイルを完全に削除します。

FTP サーバにログインした後のみ実行できます。

この動作を実行するため、FTP サーバの削除権限が必要です。

例

ファイル b.txt を削除します。

ftp> delete b.txt

```
250 Deleted b.txt
```

4.1.10 dir

Syntax

dir [*remotefile* [*localfile*]]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのファイルあるいはディレクトリを指定します。

localfile: 表示された情報が保存されるローカルファイルの名前を指定します。

説明

dir コマンドは FTP サーバ上の、現在のディレクトリにあるファイルおよびサブディレクトリに関する詳細情報を表示します。

dir *remotefile* コマンドは FTP サーバのファイルあるいはディレクトリに関する詳細情報を表示します。

dir *remotefile localfile* コマンドはリモート FTP サーバ上の指定したファイルまたはディレクトリに関する詳細情報を表示し、表示された情報を引数 *localfile* で指定したローカルファイルに保存します。

FTP サーバにログインした後のみ実行できます。

FTP client view において、**dir** コマンドは **ls** コマンドと同一です。

例

FTP サーバの現在のディレクトリのファイル、サブディレクトリの詳細情報を表示します。

ftp> dir

```
150 Connecting to port 50201
-rwxr-xr-x    1 0        0             1481 Jul  7 15:36 a.txt
drwxr-xr-x    2 0        0             8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0        0             8192 Jul  7 15:21 ftp
drwxr-xr-x    2 0        0             8192 Jul  5 09:15 logfile
-rwxr-xr-x    1 0        0             3050 Jul  7 12:26 startup.cfg
-rwxr-xr-x    1 0        0            54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0        0             1481 Jul  7 12:34 x.cfg
226 7 matches total
```

関連コマンド

ls

4.1.11 disconnect

Syntax

disconnect

View

FTP client view

定義済みユーザロール

network-admin

説明

disconnect コマンドは FTP client view から移動することなく、FTP サーバへの接続を終了します。

FTP サーバにログインした後のみ実行できます。

例

FTP client view から移動することなく、FTP サーバへの接続を終了します。

ftp> disconnect

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
ftp>
```

関連コマンド

close

4.1.12 display ftp client source

Syntax

display ftp client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ftp client source コマンドは FTP クライアントの設定の送信元アドレスを表示します。

例

FTP クライアントの設定の送信元アドレスを表示します。

<AP> display ftp client source

```
The source IP address of the FTP client is 1.1.1.1.
The source IPv6 address of the FTP client is 2001::1.
```

4.1.13 ftp

Syntax

ftp [*ftp-server* [*service-port*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]] *

View

User view

定義済みユーザロール

network-admin

パラメータ

ftp-server: FTP サーバの IPv4 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

service-port: FTP サーバの TCP ポート番号を指定します。設定範囲は 0～65535 です。デフォルトは 21 です。

dscp *dscp-value*: 送信 FTP パケットで使用される IPv4 パケットの DSCP 値です。パケットの優先度を示します。設定範囲は 0～63 です。デフォルトは 0 です。

source { **interface** *interface-type interface-number* | **ip** *source-ip-address* }: FTP 接続を確立するために使用する送信元アドレスを指定します。

- **interface** *interface-type interface-number*: インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは FTP パケットを送信する送信元アドレスとして使用されます。送信元インタフェースにプライマリ IPv4 アドレスが設定されていない場合、接続は確立できません。
- **ip** *source-ip-address*: IPv4 アドレスを指定します。すでに装置で設定されている必要があります。

説明

ftp コマンドは FTP サーバにログインし、FTP client view に移行します。

このコマンドは IPv4 ネットワークでのみ有効です。

パラメータが指定されない場合、FTP サーバにログインしないで FTP client view に移行します。

パラメータが指定されている場合、FTP にログインするためのユーザ名とパスワードを入力する画面が表示されます。

例

FTP サーバ 192.168.0.211 にログインします。

<AP>ftp 192.168.0.211

```
Press CTRL+C to abort.
Connected to 192.168.0.211 (192.168.0.211).
220 3Com 3CDaemon FTP Server Version 2.0
User (192.168.0.211:(none)): abc
331 User name ok, need password
Password:
230 User logged in
Remote system type is UNIX.
Using binary mode to transfer files.
```

ftp>

4.1.14 ftp client source

Syntax

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

undo ftp client source

デフォルト

FTP パケットを送信する送信元 IPv4 アドレスは設定されていません。装置は送信元 IP アドレスとしてルートの送信インタフェースのプライマリ IPv4 アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: FTP 接続を確立する送信元インタフェースを指定します。送信元インタフェースのプライマリ IPv4 アドレスは FTP サーバに送信するパケットの送信元 IP アドレスとして使用されます。転送が成功するために、インタフェースが UP し、プライマリ IPv4 アドレスが設定されていることを確認してください。

ip *source-ip-address*: FTP パケットを送信する送信元 IP アドレスを指定します。UP 状態のインタフェースの IPv4 アドレスが設定されていることを確認してください。そうでなければ転送が失敗します。

説明

ftp client source コマンドは FTP パケットを送信する送信元 IPv4 アドレスを指定します。

undo ftp client source コマンドはデフォルトに戻します。

このコマンドを複数実行した場合、最後に実行したコマンドが適用されます。

ftp コマンドで送信元アドレスが指定されている場合、**ftp client source** コマンドで指定された送信元アドレスよりも優先されます。

ftp client source コマンドで指定された送信元アドレスはすべての FTP 接続に適用されます。**ftp** コマンドで指定された送信元アドレスは現在の FTP 接続に適用されます。

例

FTP パケットを送信する送信元 IPv4 アドレスとして 192.168.20.222 を指定します。

<AP> system-view

[AP] ftp client source ip 192.168.20.222

関連コマンド

ftp

4.1.15 get

Syntax

get *remotefile* [*localfile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: ダウンロードするファイル名を指定します。

localfile: ダウンロードされたファイルの名前を指定します。指定しない場合、ダウンロードするファイル名を使用します。

説明

get コマンドは FTP サーバからファイルをダウンロードし、ファイルに保存します。

FTP サーバにログインしたのち、このコマンドを行うことができます。

ftp コマンドによって作業ディレクトリにダウンロードされたファイルを保存するため、以下のどちらかの作業を行います。

- *localfile* パラメータを指定しない場合、元のファイル名を使用します。
- *localfile* パラメータを指定する場合、ファイル名にパス情報を入力しないでください。たとえば a.cfg です。

ダウンロードされたファイルをほかのディレクトリに保存する場合、*localfile* パラメータはターゲットディレクトリと flash:/subdirectory/a.cfg のようなファイル名を追加する必要があります。

例

ファイル a.txt をダウンロードし、b.txt として **ftp** コマンドの作業ディレクトリに保存します。

ftp> get a.txt b.txt

```
local: b.txt remote: a.txt
150 Connecting to port 47457
226 File successfully transferred
1569 bytes received in 0.00527 seconds (290.6 kbyte/s)
```

関連コマンド

put

4.1.16 help

Syntax

help [*command-name*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

command-name: FTP クライアントでサポートされるコマンドを指定します。

説明

help コマンドは FTP クライアントでサポートされるすべてのコマンドを表示します。

help *command-name* コマンドはコマンドのヘルプ情報を表示します。

FTP client view において **help** コマンドは、**?**コマンドと同一です。

例

FTP クライアントでサポートされるすべてのコマンドを表示します。

ftp> help

```
Commands may be abbreviated.  Commands are:

append          delete          ls              quit            rmdir
ascii           debug           mkdir           reget           status
binary          dir             newer           rstatus         system
bye             disconnect      open            rhelp           user
cd              get             passive         rename          verbose
cdup            help            put             reset           ?
close           lcd             pwd             restart
```

dir コマンドのヘルプ情報を表示します。

ftp> help dir

```
dir             list contents of remote directory
```

関連コマンド

?

4.1.17 lcd

Syntax

lcd [*directory* | **/**]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: FTP クライアントのローカルディレクトリを指定します。/flash:/logfile のように記憶媒体の名前の前にスラッシュ（/）が必要です。

/: FTP クライアントのルートディレクトリを指定します。

説明

lcd コマンドは FTP クライアントのローカル作業ディレクトリを表示します。

lcd *directory* コマンドは FTP クライアントのローカル作業ディレクトリを指定したディレクトリに変更します。

lcd /コマンドは FTP クライアントのローカル作業ディレクトリをローカルルートディレクトリに変更します。

例

ローカル作業ディレクトリを表示します。

ftp> lcd

```
Local directory now /flash:
```

ローカル作業ディレクトリを flash:/logfile に変更します。

ftp> lcd /flash:/logfile

```
Local directory now /flash:/logfile
```

4.1.18 ls

Syntax

ls [*remotefile* [*localfile*]]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのファイルあるいはディレクトリを指定します。

localfile: 表示された情報が保存されるローカルファイルの名前を指定します。

説明

ls コマンドは FTP サーバ上の、現在のディレクトリにあるファイルおよびサブディレクトリに関する詳細情報を表示します。

ls *remotefile* コマンドは FTP サーバのファイルあるいはディレクトリに関する詳細情報を表示します。

ls *remotefile localfile* コマンドはリモート FTP サーバ上の指定したファイルまたはディレクトリに関する詳細情報を表示し、表示された情報を引数 *localfile* で指定したローカルファイルに保存します。

FTP サーバにログインした後のみ実行できます。

FTP client view において、**ls** コマンドは **dir** コマンドと同一です。

例

FTP サーバの現在のディレクトリのファイル、サブディレクトリの詳細情報を表示します。

ftp> ls

```
150 Connecting to port 50201
-rwxr-xr-x    1 0        0              1481 Jul  7 15:36 a.txt
-rwxr-xr-x    1 0        0                 0 Sep 27  2010 base.bin
drwxr-xr-x    2 0        0              8192 Jul  2 14:33 diagfile
drwxr-xr-x    3 0        0              8192 Jul  7 15:21 ftp
-rwxr-xr-x    1 0        0                 0 Sep 27  2010 kernel.bin
drwxr-xr-x    2 0        0              8192 Jul  5 09:15 logfile
drwxr-xr-x    2 0        0              8192 Jul  2 14:33 seclog
-rwxr-xr-x    1 0        0          40808448 Jul  2 14:33 simware-cmw710-sys
tem-a1801.bin
-rwxr-xr-x    1 0        0              3050 Jul  7 12:26 startup.cfg
```

```
-rwxr-xr-x    1 0        0             54674 Jul  4 09:24 startup.mdb
-rwxr-xr-x    1 0        0              1481 Jul  7 12:34 x.cfg
226 11 matches total
```

ファイル a.txt の詳細情報を s.txt に保存します。

ftp> ls a.txt s.txt

```
output to local-file: s.txt ? [Y/N]y
150 Connecting to port 50203
226-Glob: s.txt
```

ファイル s.txt の内容を表示します。

ftp> bye

```
221-Goodbye. You uploaded 0 and downloaded 2 kbytes.
221 Logout.
```

<AP> more s.txt

```
-rwxr-xr-x    1 0        0              1481 Jul  7 12:34 a.txt
```

関連コマンド

dir

4.1.19 mkdir

Syntax

mkdir *directory*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: 作成するディレクトリの名前を指定します。

説明

mkdir コマンドは FTP サーバの現在のディレクトリにサブディレクトリを作成します。

FTP サーバにログインした後のみ実行できます。

この動作を実行するため、FTP サーバの権限が必要です。

例

リモート FTP サーバの現在のディレクトリにサブディレクトリ newdir を作成します。

ftp> mkdir newdir

```
257 "newdir" : The directory was successfully created
```

4.1.20 newer

Syntax

newer *remotefile* [*localfile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

remotefile: FTP サーバのリモートファイルの名前を指定します。

localfile: アップデートされたローカルファイルの名前を指定します。

説明

newer コマンドは FTP サーバのリモートファイルをローカルファイルにアップデートします。

FTP サーバにログインした後のみ実行できます。

ローカルファイルが存在しない場合、FTP サーバからファイルをダウンロードし、ローカルに保存します。

FTP サーバのリモートファイルがローカルファイルよりも古い場合、ローカルファイルをアップデートしません。

例

FTP サーバのファイル a.txt をローカルファイルにアップデートします。

ftp> newer a.txt

```
local: a.txt remote: a.txt
150 Connecting to port 63513
226 File successfully transferred
1573 bytes received in 0.0293 seconds (52.3 kbyte/s)
```

4.1.21 open

Syntax

open *server-address* [*service-port*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

server-address: FTP サーバの IP アドレスまたはホスト名を指定します。

service-port: FTP サーバの TCP ポート番号を指定します。設定範囲は 0～65535 です。デフォルトは 21 です。

説明

open コマンドは FTP client view で FTP サーバにログインします。

このコマンドを実行した後、システムはユーザ名とパスワードを入力する画面が表示されます。

ある FTP サーバにログインした後、別のサーバに **open** コマンドを使用してログインする前に、サーバから切断する必要があります。

例

FTP client view で FTP サーバ 192.168.40.7 にログインします。

<AP>ftp

```
ftp> open 192.168.40.7
Press CTRL+C to abort.
Connected to 192.168.40.7 (192.168.40.7).
220 FTP service ready.
User (192.168.40.7:(none)): root
331 Password required for root.
Password:
230 User logged in.
Remote system type is NEC.
ftp>
```

4.1.22 passive

Syntax

passive

デフォルト

passive

View

FTP client view

定義済みユーザロール

network-admin

説明

passive コマンドは FTP 伝送モードを passive に設定します。

ftp は以下のいずれかのモードを実行することができます。

- **Active モード**—FTP サーバが TCP 接続を開始します。
- **Passive モード**—FTP クライアントが TCP 接続を開始します。

このコマンドはモードの切り替えを行うため、複数回実行することができます。

このコマンドは主にプライベートネットワークユーザとパブリックネットワークユーザ間の FTP セッションの確立を制御する Firewall と一緒に使用されます。

例

FTP 伝送モードを passive に設定します。

ftp> passive

```
Passive mode on.
```

ftp> passive

```
Passive mode off.
```

4.1.23 put

Syntax

put *localfile* [*remotefile*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

localfile: アップロードするファイル名を指定します。

remotefile: FTP サーバでアップロードされたファイルを保存するファイル名を指定します。

説明

put コマンドはリモート FTP クライアントから FTP サーバにファイルをアップロードします。

FTP サーバにログインした後のみ実行できます。

ftp コマンドによって作業ディレクトリにアップロードするため、*localfile* パラメータで a.cfg のようなファイル名を指定する必要があります。

アップロードされたファイルをほかのディレクトリに保存する場合、*localfile* パラメータはターゲットディレクトリと flash:/subdirectory/a.cfg のようにファイル名を追加する必要があります。

例

ftp コマンドで作業ディレクトリにファイル a.txt をアップロードします。FTP サーバに b.txt として保存します。

ftp> put a.txt b.txt

```
local: a.txt remote: b.txt
150 Connecting to port 47461
226 File successfully transferred
1569 bytes sent in 0.000671 seconds (2.23 Mbyte/s)
```

関連コマンド

get

4.1.24 pwd

Syntax

pwd

View

FTP client view

定義済みユーザロール

network-admin

説明

pwd コマンドは FTP サーバの現在アクセスしているディレクトリを表示します。

FTP サーバにログインした後のみ実行できます。

例

リモート FTP サーバの現在アクセスしているディレクトリを表示します。

ftp> cd subdir

```
250 OK. Current directory is /subdir
```

ftp> pwd

```
257 "/subdir" is your current location
```

4.1.25 quit

Syntax

quit

View

FTP client view

定義済みユーザロール

network-admin

説明

quit コマンドは FTP サーバの接続を終了し、user view に戻ります。

例

FTP サーバの接続を終了し、user view に戻ります。

ftp> quit

```
221-Goodbye. You uploaded 0 and downloaded 0 kbytes.
221 Logout.
<AP>
```

関連コマンド

bye

4.1.26 rhelp

Syntax

rhelp [*protocol-command*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

protocol-command: FTP 関連コマンドを指定します。

説明

rhelp コマンドは FTP サーバがサポートしている FTP 関連コマンドを表示します。

rhelp *protocol-command* コマンドは FTP サーバがサポートしている FTP 関連コマンドのヘルプ情報を表示します。

FTP サーバにログインした後のみ実行できます。

例

FTP サーバがサポートしている FTP 関連コマンドを表示します。

ftp> rhelp

```
214-The following FTP commands are recognized
 USER PASS NOOP QUIT SYST TYPE
 HELP CWD  XCWD PWD  CDUP XCUP
 XPWD LIST NLST MLSD PORT EPRT
 PASV EPSV REST RETR STOR APPE
 DELE MKD  XMKD RMD  XRMD ABOR
 SIZE RNFR RNTO
214 UNIX Type: L8
```

表 4-1 コマンド出力

フィールド	説明
USER	ユーザ名を表示します。
PASS	パスワードを表示します。
NOOP	Null動作です。
SYST	システムパラメータを表示します。
TYPE	要求タイプを表示します。
CWD	現在のディレクトリを変更します。
XCWD	CWDコマンドの拡張コマンドです。
PWD	現在のディレクトリを表示します。
CDUP	上位ディレクトリに移動します。
XCUP	CDUPコマンドの拡張コマンドです。
XPWD	PWDコマンドの拡張コマンドです。
LIST	ファイルリストを表示します。
NLST	ファイルの説明を概要表示します。
MLSD	ファイル内容を表示します。

フィールド	説明
PORT	アクティブモード（IPv4）です。
EPRT	アクティブモード（IPv6）です。
PASV	パッシブモード（IPv4）です。
EPSV	パッシブモード（IPv6）です。
REST	再起動します。
RETR	ファイルをダウンロードします。
STOR	ファイルをアップロードします。
APPE	アップロードを追記します。
DELE	ファイルを削除します。
MKD	フォルダを作成します。
XMKD	MKDコマンドの拡張コマンドです。
RMD	フォルダを削除します。
XRMD	RMDコマンドの拡張コマンドです。
ABOR	転送を中断します。
SIZE	転送ファイルのサイズを表示します。
RNFR	元の名前を表示します。
RNTO	新しい名前を表示します。

4.1.27 rmdir

Syntax

rmdir *directory*

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

directory: リモート FTP サーバのディレクトリ名を指定します。

説明

rmdir コマンドは FTP サーバのディレクトリを完全に削除します。

FTP サーバにログインした後のみ実行できます。

この動作を実行するため、FTP サーバの削除権限が必要です。

ディレクトリを削除する前に、ディレクトリにあるすべてのファイルとサブディレクトリを削除する必要があります。ファイルを削除する方法については、**delete** コマンドを参照してください。

コマンドを実行すると、指定したディレクトリのごみ箱にあるファイルは削除しません。

例

空のディレクトリ subdir1 を削除します。

ftp> rmdir subdir1

```
250 The directory was successfully removed
```

関連コマンド

delete

4.1.28 user

Syntax

user *username* [*password*]

View

FTP client view

定義済みユーザロール

network-admin

パラメータ

username: ターゲットユーザアカウントのユーザ名を指定します。

password: ターゲットユーザアカウントのパスワードを指定します。

説明

user コマンドは現在の FTP 接続で FTP 認証を初期化します。

FTP サーバにアクセスしようとして認証に失敗した場合、FTP サーバへの接続が終了する前に再度アクセスすることができます。

FTP サーバにログイン後、新しいアカウントに FTP 認証を開始することができます。

新しいアカウントに変更することで、FTP 接続を再確立することなく、異なる権限を取得することができます。

ターゲットユーザアカウントのユーザ名とパスワードは設定されている必要があります。そうでなければ、ユーザアカウントの変更は失敗し、FTP 接続が切断されます。

例

FTP にログインしたのち、ユーザ名 ftp、パスワード 123456 を使用し、FTP サーバにログインします。（出力は FTP サーバによって変わる可能性があります）

- 方法 1:

ftp> user ftp 123456

```
331 Password required for ftp.
230 User logged in.
```

- 方法 2:

ftp> user ftp

```
331 Password required for ftp.
Password:
230 User logged in.
```

4.1.29 verbose

Syntax

verbose

デフォルト

装置は FTP 動作の詳細情報を表示します。

View

FTP client view

定義済みユーザロール

network-admin

説明

verbose コマンドは FTP 動作の詳細情報の表示機能を有効、あるいは無効にします。

このコマンドは現在のセッションのみ適用されます。再度ログインしたとき、デフォルトの設定に戻ります。

例

FTP 動作の詳細情報の表示機能を無効にします。

ftp> verbose

```
Verbose mode off.
```

get コマンドを実行します。

ftp> get a.cfg 1.cfg

FTP 動作の詳細情報の表示機能を有効にします。

ftp> verbose

```
Verbose mode on.
```

get コマンドを実行します。

ftp> get a.cfg 2.cfg

```
227 Entering Passive Mode (192,168,1,58,68,14)
150-Accepted data connection
150 The computer is your friend. Trust the computer
226 File successfully transferred
3796 bytes received in 0.00762 seconds (486.5 kbyte/s)
```

4.2 TFTPクライアント設定コマンド

4.2.1 tftp

Syntax

tftp *tftp-server* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**dscp** *dscp-value* | **source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

tftp-server: TFTP サーバの IPv4 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字で、大文字、小文字を区別しません。ホスト名で使用できる文字列は英字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

get: ファイルをダウンロードし、宛先ファイルにファイルのディレクトリを書き込みます。宛先ファイルがすでに存在する場合、システムはダウンロードを開始する前に既存のファイルを削除します。ダウンロードが失敗しても既存のファイルは完全に削除されます。

put: ファイルをアップロードします。

sget: ファイルをダウンロードし、宛先ファイルを書き込みする前に、メモリにファイルを保存します。ダウンロードされたファイルが正常にメモリにダウンロードされたのち宛先ファイルにダウンロードされたファイルの書き込みを行います。宛先ファイルがすでに存在する場合、ダウンロードされたファイルは既存のファイルに上書きします。ダウンロードあるいはメモリへの書き込みが失敗すると、既存のファイルは上書きされません。

source-filename: 送信元ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。

destination-filename: 宛先ファイル名を指定します。設定範囲は 1～255 文字で、大文字、小文字を区別しません。この引数が指定されない場合、ファイルは送信元ファイル名を使用します。

dscp *dscp-value*: 送信する TFTP パケットの IPv4 パケットの DSCP 値です。パケットを転送する優先度を示します。設定範囲は 0～63 です。デフォルトは 0 です。

source { **interface** *interface-type interface-number* | ip *source-ip-address* }: 送信する TFTP パケットの送信元アドレスを指定します。キーワードが指定されない場合、装置は送信元 IPv4 アドレスとして TFTP サーバへのルートの出力インタフェースのプライマリ IPv4 アドレスを使用します。

- **interface** *interface-type interface-number*: インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは送信する TFTP パケットの送信元 IPv4 アドレスとして使用されます。インタフェースが UP でプライマリ IPv4 アドレスが設定されている必要があります。そうでなければ転送が失敗します。
- **ip** *source-ip-address*: IPv4 アドレスを指定します。インタフェースが UP でアドレスが IPv4 アドレスである必要があります。そうでなければ転送が失敗します。

説明

tftp コマンドは TFTP サーバからファイルをダウンロードあるいは IPv4 ネットワークの TFTP サーバにファイルをアップロードします。

tftp コマンドで指定された送信元アドレスは **tftp client source** コマンドで指定された送信元アドレスよりも優先されます。

tftp client source コマンドで指定された送信元アドレスはすべての TFTP 接続に適用されます。**tftp** コマンドで指定された送信元アドレスは現在の TFTP 接続に適用されます。

例

TFTP サーバ 192.168.1.1 から new.bin ファイルをダウンロードし、new.bin として保存します。

<AP> tftp 192.168.1.1 get new.bin

```
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 13.9M  100 13.9M    0     0  1206k      0  0:00:11  0:00:11 --:--:-- 1206k
Writing file...Done.
```

<AP>

表 4-2 コマンド出力

フィールド	説明
%	ファイル転送の進捗状況を%で示します。
Total	転送されたファイルサイズです。単位はbyteです。
%	全ファイルサイズに対する受信したファイルサイズの割合を%で示します。
Received	受信したファイルサイズです。単位はbyteです。
%	全ファイルサイズに対する送信したファイルサイズの割合を%で示します。
Xferd	送信したファイルサイズです。単位はbyteです。
Average Dload	平均ダウンロード速度です。単位はbpsです。

フィールド	説明
Speed Upload	平均アップロード速度です。単位はbpsです。
Writing file...	システムがダウンロードファイルを記憶媒体に書き込みを行っています。**get**パラメータあるいは**sget**パラメータを指定したときのみ表示されます。 処理が成功すると、フィールドの最後に**Done**と表示します。 処理が失敗すると、フィールドの最後に**Failed**と表示します。

関連コマンド

tftp client source

4.2.2 tftp client source

Syntax

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

undo tftp client source

デフォルト

TFTP サーバに送信する TFTP パケットで設定された送信元 IPv4 アドレスはありません。装置はルートの出力インタフェースのプライマリ IPv4 アドレスを送信元 IP アドレスとして使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 確立する TFTP 接続の送信元インタフェースを指定します。送信元インタフェースのプライマリ IPv4 アドレスは TFTP サーバに送信されるパケットの送信元 IPv4 アドレスとして使用されます。インタフェースが UP でプライマリ IPv4 アドレスが設定されている必要があります。そうでなければ転送が失敗します。

ip *source-ip-address*: 送信する TFTP パケットの送信元 IPv4 アドレスを指定します。UP 状態のインタフェースのアドレスが IPv4 アドレスである必要があります。そうでなければ転送が失敗します。

説明

tftp client source コマンドは TFTP サーバに送信する TFTP パケットの送信元 IPv4 アドレスを指定します。

undo tftp client source コマンドはデフォルトに戻します。

このコマンドを複数実行した場合、最後に実行したコマンドが適用されます。

tftp コマンドで送信元アドレスが指定されている場合、**tftp client source** コマンドで指定された送信元アドレスよりも優先されます。

tftp client source コマンドで指定された送信元アドレスはすべての TFTP 接続に適用されます。**tftp** コマンドで指定された送信元アドレスは現在の TFTP 接続に適用されます。

例

TFTP サーバに送信する TFTP パケットの送信元 IP アドレスを 192.168.20.222 として指定します。

<AP> system-view

[AP] tftp client source ip 192.168.20.222

関連コマンド

tftp

4.2.3 tftp-server acl

Syntax

tftp-server acl *acl-number*

undo tftp-server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

acl-number: 標準 ACL の番号を指定します。設定範囲は 2000～2999 です。

説明

tftp-server acl コマンドは IPv4 ネットワークの TFTP サーバへの装置のアクセスを制御する ACL を使用します。

undo tftp-server acl コマンドはデフォルトに戻します。

ACL を使用して、装置から指定された TFTP サーバへのアクセスを許可または禁止することができます。

例

TFTP サーバ 1.1.1.1 へのアクセスのみを許可します。

<AP> system-view

[AP] acl basic 2000

[AP-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0

[AP-acl-ipv4-basic-2000] quit

[AP] tftp-server acl 2000

目次

このセクションのページは **1-x-x** です。

5 章 ファイルシステム管理 5-1
5.1 ファイルシステム管理設定コマンド 5-1
5.1.1 cd 5-2
5.1.2 copy 5-3
5.1.3 delete 5-5
5.1.4 dir 5-7
5.1.5 file prompt 5-10
5.1.6 fixdisk 5-11
5.1.7 format 5-12
5.1.8 gunzip 5-12
5.1.9 gzip 5-14
5.1.10 mkdir 5-14
5.1.11 more 5-16
5.1.12 move 5-16
5.1.13 pwd 5-18
5.1.14 rename 5-19
5.1.15 reset recycle-bin 5-20
5.1.16 rmdir 5-21
5.1.17 tar create 5-21
5.1.18 tar extract 5-23
5.1.19 tar list 5-25
5.1.20 undelete 5-25

5章 ファイルシステム管理

5.1 ファイルシステム管理設定コマンド

⚠ **注意**：

- 記録媒体、ファイル、ディレクトリを管理する前に、設定が装置に与える影響を確認してから行ってください。
- ピリオド（．）の名前で始まるファイルあるいはディレクトリは、隠しファイルあるいは隠しディレクトリです。ファイルあるいはディレクトリの先頭にピリオド（．）を使用しないでください。
- いくつかの隠しファイルと隠しディレクトリが存在します。ファイルシステムの管理を行う際は、隠しファイルや隠しディレクトリを修正しないでください。

⚠ **注意**：

- 表示される空き容量は実際のファイルサイズで計算されています。保存に必要なサイズはファイルの種類によって実際のファイルサイズと異なる場合がありますので、ファイルの保存は十分な空き容量があることを確認してから行ってください。
- ファイルのダウンロードやコピーを行う場合は、十分な空き容量を確保してから行ってください。空き容量が不足している場合には、エラーとなり異常なファイルが残る場合があります。保存に失敗した場合は、不要なファイルを削除してください。

ファイルシステムはフラッシュメモリなどの記憶媒体です。

ファイル名、ディレクトリ名はファイル名のフォーマットで指定されています。詳細はオペレーションマニュアルのセクション 1 *基本機能 “ファイルシステム管理”*を参照してください。

ファイルシステムでのコピー、削除、フォーマット、ファイルの圧縮、解凍、ディレクトリの作成、移動、ファイル名の変更、ディレクトリの削除、ファイルの復元を行う前に、フラッシュメモリのプロテクトが解除されていることを確認してください。

別のユーザがファイルシステムの回復、フォーマットを行っている間、ファイルシステムにアクセスすることはできません。

ファイルシステムの回復、フォーマットの後、ファイルシステムにアクセスする場合、以下のいずれかの作業を行ってください。

- コマンドのファイルシステムの名前を指定してください。たとえば、フラッシュメモリのすべてのファイル、ディレクトリを表示する **dir flash:/**コマンドを使用してください。
- コマンドを使用する前に、ファイルシステムにディレクトリを変更する場合、**cd** コマンドを使用してください。たとえば、フラッシュメモリのルートディレクトリに移動する場合、コ **cd flash:/**コマンドを使用してください。そしてすべてのファイル、ディレクトリを表示するために **dir** コマンドを使用してください。

5.1.1 cd

Syntax

cd { *directory* | **..** }

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: 宛先ディレクトリの名前を指定します。

..: 上位ディレクトリに戻ります。現在のディレクトリがルートディレクトリである場合、コマンドを実行したときエラーメッセージが表示されます。このパラメータに対するコマンドラインヘルプはありません。

説明

cd コマンドは現在の作業ディレクトリを変更します。

例

装置にログインした後、ディレクトリ test にアクセスします。

<AP> cd test

上位ディレクトリに戻ります。

<AP> cd ..

5.1.2 copy

Syntax

copy *source-file* { *dest-file* | *dest-directory* } [**source interface** *interface-type interface-number*] [append]

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file: ファイルの名前あるいは URL を指定します。ファイルが装置上ではなく FTP、TFTP サーバにある場合、ファイル URL を指定します。URL が大文字、小文字を区別するかどうかはサーバによって異なります。

{ *dest-file* | *dest-directory* }: 宛先ファイルの名前あるいは URL を指定します。送信元ファイルを FTP あるいは TFTP サーバにコピーする場合、URL を指定します。ディレクトリを指定する場合、装置は指定したファイルをディレクトリにコピーしもとのファイル名で保存します。URL が大文字、小文字を区別するかどうかはサーバによって異なります。

source interface *interface-type interface-number*: サーバに接続するために使用される送信元インタフェースを指定します。送信元インタフェースを指定すると、装置外部向けパケットの送信元 IP アドレスとして、装置は送信元インタフェースのプライマリ IP アドレスを使用します。本オプションを指定しなかった場合、装置は送信元インタフェースとして外向きインタフェースを使用します。

append: 送信失敗や中断が発生した場合に、正しく送信された内容を保存し、再度コマンドを実行したときに欠落部分をコピーし続けます。このパラメータを指定しない場合、送信失敗または中断が発生した場合、デバイスは正しく送信されたコンテンツを破棄します。このパラメータは、FTP または HTTP ファイル サーバとの間でファイルをコピーする場合にのみサポートされます。

説明

copy コマンドはファイルをコピーします。

以下の処理を実行することができます。

- ローカルファイルをコピーし、ローカルに保存します。
- ローカルファイルをコピーし、FTP あるいは TFTP サーバに保存します。
- FTP あるいは TFTP サーバのファイルをコピーし、ローカルに保存します。

ファイルあるいはディレクトリを指定するため、以下のガイドラインを使用します。

位置	フォーマット	補足
装置	オペレーションマニュアルのセクション1 *基本機能“ファイルシステム管理”の“ファイルシステムの管理の制限とガイドライン”*を参照してください。	ー
FTPサーバ	以下の形式のURLを入力します。 **ftp**://FTP *username*[:*password*]@*server address*[:*port number*]/*file path*[/*file name*].	ユーザ名とパスワードはFTPサーバで設定されているユーザ名とパスワードと同一にしてください。 サーバがユーザ名のみでユーザを認証する場合、パスワードを入力する必要はありません。 たとえばユーザ名1、パスワード1、FTPサーバ1.1.1.1で許可された作業ディレクトリのstartup.cfgを指定する場合、ftp://1:1@1.1.1.1/startup.cfgを入力します。
TFTPサーバ	以下の形式のURLを入力します。 **tftp**://*server address*[:*port number*]/*file path*[/*file name*].	たとえば、TFTPサーバ1.1.1.1の作業ディレクトリのstartup.cfgをしている場合、tftp://1.1.1.1/startup.cfgを入力します。

例

現在のディレクトリのファイル test.cfg をコピーし、ファイル名を testbackup.cfg として現在のディレクトリに保存します。

<AP> copy test.cfg testbackup.cfg

```
Copy flash:/test.cfg to flash:/testbackup.cfg? [Y/N]:y
Copying file flash:/test.cfg to flash:/testbackup.cfg...Done.
```

5.1.3 delete

Syntax

delete [**/unreserved**] *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

/unreserved: 指定されたファイルを完全に削除します。このパラメータを指定しない場合、ごみ箱にファイルを移動します。

file: 削除するファイル名を指定します。アスタリスク（*）はワイルドカードとして使用できます。たとえば、現在のディレクトリにある拡張子が”.txt”のファイルを削除する場合、”*.txt”と入力します。

説明

delete コマンドはファイルを削除します。

delete /unreserved *file* コマンドを使用する場合、削除されたファイルを復元することができません。

/unreserved パラメータを使用しないで **delete** *file* コマンドは指定したファイルをごみ箱に移動します。システムが記憶領域を使い切っていた場合、本コマンドはファイルを永久に削除します。

ごみ箱に移動したファイルは **undelete** コマンドを使用して復元することができます。

ごみ箱のファイルを削除する際に **delete** コマンドを使用しないでください。ごみ箱のファイルを削除する場合、**reset recycle-bin** コマンドを使用してください。

異なるディレクトリにある同一ファイル名の 2 つのファイルを削除する場合、2 つのファイルはごみ箱に保存されます。同一ディレクトリの同一ファイル名の 2 つのファイルを削除した場合、最後に削除されたファイルのみがごみ箱に保存されています。

例

現在のディレクトリからファイル 1.cfg を削除します。

<AP> delete 1.cfg

```
Delete flash:/1.cfg? [Y/N]:y
Deleting file flash:/1.cfg...Done.
```

現在のディレクトリからファイル 1.cfg を完全に削除します。

<AP> delete /unreserved 1.cfg

```
The file cannot be restored. Delete flash:/1.cfg? [Y/N]:y
```

```
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/1.cfg...Done.
```

関連コマンド

reset recycle-bin

undelete

5.1.4 dir

Syntax

dir [**/all**] [*file* | *directory* | **/all-filesystems**]

View

User view

定義済みユーザロール

network-admin

パラメータ

/all: 現在のディレクトリのすべてのファイルとディレクトリを隠しファイル、隠しディレクトリを含めてすべて表示します。このパラメータを指定しない場合、隠しファイル、隠しディレクトリを除いたファイルとディレクトリが表示されます。

file: 指定したファイルを表示します。アスタリスク（*）はワイルドカードとして使用できます。たとえば、現在のディレクトリにある拡張子が“.txt”のファイルを表示する場合、**dir** **.txt* と入力します。

directory: 指定したディレクトリを表示します。

/all-filesystems: 装置のすべてのファイルシステムのルートディレクトリのファイルとディレクトリを表示します。

説明

dir コマンドはファイルあるいはディレクトリを表示します。

パラメータを指定しない場合、現在のディレクトリの隠しファイル、隠しディレクトリを除いたファイルとディレクトリを表示します。

ごみ箱のディレクトリ名は“.trash”です。ごみ箱のファイルを表示する場合、以下のどちらかの方法を使用します。

- **dir /all** *.trash* コマンドを実行します。
- **cd** *.trash* コマンドを実行し、**dir** コマンドを実行します。

例

現在のディレクトリにあるすべてのファイルとディレクトリを表示します。

<AP> dir /all

```
Directory of flash: (YAFFS2)
. . .
  0 -rw- xxxxx Jan 01 2024 00:00:00 xxxxxx.xxx
  1 -rw- xxxxx Jan 01 2024 00:00:00 xxxxxx.xxx
  2 -rw- xxxxx Jan 01 2024 00:00:00 xxxxxx.xxx
. . .

xxxxx KB total (xxxxx KB free. remaining xx.xx%)
```

装置のすべてのファイルシステムのルートディレクトリにあるすべてのファイルとディレクトリを表示します。

<AP> dir /all-filesystems

```
Directory of flash: (YAFFS2)
. . .
0 -rw- xxxxx Jan 01 2024 00:00:00 xxxxxx.xxx
1 -rw- xxxxx Jan 01 2024 00:00:00 xxxxxx.xxx
2 -rw- xxxxx Jan 01 2024 00:00:00 xxxxxx.xxx
. . .
xxxxx KB total (xxxxx KB free. remaining xx.xx%)
```

表 5-1 コマンド出力

フィールド	説明
Directory of xx (yy)	現在のディレクトリです。xx はディレクトリ名を示します。yy は現在のファイルシステムのタイプを表示します。
0 -rwh 3144 Apr 26 2024 13:45:28 xx.xx	ファイルあるいはディレクトリ情報です。 ● **0**：ファイル、またはディレクトリ番号です。システムによって自動で割り当てられます。 ● **-rwh**：ファイルあるいはディレクトリの属性です。最初の文字はディレクトリを示します。**d**はディレクトリで、ーはファイルです。2番目の文字はファイルあるいはディレクトリが読み込み可能かどうかを示します。**r**は読み込み可能です。3番目の文字はファイルあるいはディレクトリが書き込み可能かどうかを示します。**w**は書き込み可能です。4番目の文字はファイルあるいはディレクトリが隠しファイルあるいは隠しディレクトリかどうかを示します。**h**は隠しファイルあるいは隠しディレクトリで、ーは通常のファイルあるいはディレクトリです。変更、名前の変更、隠しファイルあるいは隠しディレクトリの削除は機能に影響します。 ● **3144 :** ファイルサイズです。単位はbyteです。ディレクトリはハイフン（ー）が表示されます。 ● **Apr 26 2024 13:45:28**：ファイルあるいはディレクトリが変更された最後の日時です。 ● **xx.xx**：ファイルあるいはディレクトリ名です。

メモ：

QX-W610 では、ディレクトリ容量の表示について、バージョンごとに異なります。
v7.5.98 では、以下の表示になります。
　xxxxx KB total (xxxxx KB free)
v7.5.105 を含む以降のバージョンでは、以下の表示になります。
　xxxxx KB total (xxxxx KB free. remaining xx.xx%)

5.1.5 file prompt

Syntax

file prompt { **alert** | **quiet** }

undo file prompt

デフォルト

alert

View

System view

定義済みユーザロール

network-admin

パラメータ

alert: ファイルの破損やデータの損失など、望ましくない結果を引き起こす可能性のある操作について、システムが警告できるようにします。

quiet: ファイルあるいはディレクトリの操作に関する警告を行いません。

説明

file prompt コマンドはファイル、ディレクトリのプロンプトモードを設定します。

undo file prompt コマンドはデフォルトに戻します。

quiet モードである場合、システムはいかなるファイル操作に関しても警告を行いません。**alert** モードである場合、望ましくない結果を引き起こす可能性のある操作を中止できるように、警告を表示します。

例

ファイル、ディレクトリのプロンプトモードを alert に設定します。

<AP> system-view

[AP] file prompt alert

5.1.6 fixdisk

Syntax

fixdisk *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem: ファイルシステムの名前を指定します。値は装置の種類によって異なります。

説明

fixdisk コマンドは何らかの異常操作によりファイルシステムが使用できなくなった場合、ファイルシステムを確認し、ダメージ領域を復元します。

本コマンドは、ファイルシステムの空きスペースが使用できないあるいは異常な操作により解放されたとき、ファイルシステムを修正します。

ファイルシステムへのアクセスがないときのみ、ファイルシステムをフォーマットすることができます。

例

ファイルシステムの空きスペースを復元します。

<AP> fixdisk flash:

```
Restoring flash: may take some time...
Restoring flash:...Done.
```

5.1.7 format

Syntax

format *filesystem*

View

User view

定義済みユーザロール

network-admin

パラメータ

filesystem: ファイルシステムの名前を指定します。値は装置の種類によって異なります。

説明

format コマンドはファイルシステムをフォーマットします。

ファイルシステムをフォーマットすると、ファイルシステムにあるすべてのファイルを完全に削除します。ファイルシステムに起動設定ファイルが存在する場合は、必要であればバックアップを取ってください。

ファイルシステムへのアクセスがないときのみ、ファイルシステムをフォーマットすることができます。

例

ファイルシステムをフォーマットします。

<AP> format flash:

```
All data on flash: will be lost, continue? [Y/N]:y
Formatting flash:... Done.
```

5.1.8 gunzip

Syntax

gunzip *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: 解凍するファイルの名前を指定します。拡張子は“.gz”にする必要があります。

説明

gunzip コマンドはファイルを解凍します。

本コマンドは解凍した後、もとのファイルを削除します。

例

ファイル system.bin.gz を解凍します。

1)　ファイルを解凍する前に、system の文字列で始まる名前のファイルを表示します。

<AP> dir system.*

```
Directory of flash:
  1 -rw-        20 Jun 14 2012 10:18:53   system.bin.gz
472972 KB total (472840 KB free)
```

2)　ファイル system.bin.gz を解凍します。

<AP> gunzip system.bin.gz

```
Decompressing file flash:/system.bin.gz..... Done.
```

3)　解凍した操作の確認を行います。

<AP> dir system.*

```
Directory of flash:
  1 -rw-         0 May 30 2012 11:42:25   system.bin
472972 KB total (472844 KB free)
```

5.1.9 gzip

Syntax

gzip *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: 圧縮するファイル名を指定します。圧縮するファイルの拡張子は、“.gz”で保存されます。

説明

gzip コマンドはファイルを圧縮します。

本コマンドは圧縮した後、もとのファイルを削除します。

例

ファイル system.bin を圧縮します。

1)　ファイルを圧縮する前に、system の文字列で始まる名前のファイルを表示します。

<AP> dir system.*

```
Directory of flash:
  1 -rw-         0 May 30 2012 11:42:24   system.bin
472972 KB total (472844 KB free)
```

2)　ファイル system.bin を圧縮します。

<AP> gzip system.bin

```
Compressing file flash:/system.bin..... Done.
```

3)　圧縮した操作の確認を行います。

<AP> dir system.*

```
Directory of flash:
  1 -rw-        20 Jun 14 2012 10:18:53   system.bin.gz
472972 KB total (472840 KB free)
```

5.1.10 mkdir

Syntax

mkdir *directory*

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: ディレクトリの名前を指定します。

説明

mkdir コマンドは現在のディレクトリの下にディレクトリを作成します。

ディレクトリの名前は指定されたディレクトリ内で一意にする必要があります。

既に存在するディレクトリに対してのみ新しいディレクトリを作成可能です。たとえば、ディレクトリ flash:/test/mytest を作成する場合、ディレクトリ test は既に存在している必要があります。

例

現在のディレクトリにディレクトリ test を作成します。

<AP> mkdir test

```
Creating directory flash:/test... Done.
```

現在のディレクトリにディレクトリ test/subtest を作成します。

<AP> mkdir test/subtest

```
Creating directory flash:/test/subtest... Done.
```

5.1.11 more

Syntax

more *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: ファイル名を指定します。

説明

more コマンドはテキストファイルの内容を表示します。

例

ファイル test.txt の内容を表示します。

<AP> more test.txt

```
Have a nice day.
```

ファイル testcfg.cfg の内容を表示します。

<AP> more testcfg.cfg

```
#
version 7.1.064, ESS 5103
#
 sysname AP
#
  ---- More ----
```

5.1.12 move

Syntax

move *source-file* { *dest-file* | *dest-directory* }

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file: ソースファイルの名前を指定します。

dest-file: ターゲットファイルの名前を指定します。

dest-directory: ターゲットファイルあるいはディレクトリの名前を指定します。

説明

move コマンドはファイルを移動します。

ターゲットディレクトリを指定する場合、システムはファイル名を変更しないで指定したディレクトリにソースファイルを移動します。

例

ファイル flash:/test/sample.txt を flash:/に移動し、ファイル 1.txt として保存します。

<AP> move test/sample.txt 1.txt

```
Move flash:/test/sample.txt to flash:/1.txt? [Y/N]:y
Moving file flash:/test/sample.txt to flash:/1.txt ...Done.
```

ファイル b.cfg をディレクトリ test2 に移動します。

<AP> move b.cfg test2

```
Move flash:/b.cfg to flash:/test2/b.cfg? [Y/N]:y
Moving file flash:/b.cfg to flash:/test2/b.cfg... Done.
```

5.1.13 pwd

Syntax

pwd

View

User view

定義済みユーザロール

network-admin

説明

pwd コマンドは現在の作業ディレクトリを表示します。

例

現在の作業ディレクトリを表示します。

<AP> pwd

```
flash:
```

5.1.14 rename

Syntax

rename { *source-file* | *source-directory* } { *dest-file* | *dest-directory* }

View

User view

定義済みユーザロール

network-admin

パラメータ

source-file: ソースファイルの名前を指定します。

source-directory:ソースディレクトリの名前を指定します。

dest-file: ターゲットファイルの名前を指定します。

dest-directory:ターゲットディレクトリの名前を指定します。

説明

rename コマンドはファイルあるいはディレクトリの名前を変更します。

現在の作業ディレクトリのファイルあるいはディレクトリに変更しようとするファイルあるいはディレクトリの名前が存在する場合、本コマンドは実行されません。

例

ファイル copy.cfg をファイル test.cfg に変更します。

<AP> rename copy.cfg test.cfg

```
Rename flash:/copy.cfg as flash:/test.cfg? [Y/N]:y
Renaming flash:/copy.cfg as flash:/test.cfg... Done.
```

5.1.15 reset recycle-bin

Syntax

reset recycle-bin [**/force**]

View

User view

定義済みユーザロール

network-admin

パラメータ

/force: 確認のプロンプトの表示を行わず、ごみ箱のすべてのファイルを削除します。このパラメータを指定しない場合、確認のプロンプトが表示されます。

説明

reset recycle-bin コマンドはごみ箱からファイルを削除します。

delete *file* コマンドはごみ箱にファイルを移動します。ファイルを完全に削除する場合、**reset recycle-bin** コマンドを使用してごみ箱を消去します。

ファイルが壊れている場合、**reset recycle-bin** コマンドではファイルを削除できない可能性があります。その場合は、**reset recycle-bin /force** コマンドを使用します。

例

2 つのファイルが存在しているごみ箱からファイルを削除します。

<AP> reset recycle-bin

```
Clear flash:/a.cfg? [Y/N]:y
Clearing file flash:/a.cfg... Done.
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

2 つのファイルが存在しているごみ箱からファイル b.cfg を削除します。

<AP> reset recycle-bin

```
Clear flash:/a.cfg? [Y/N]:n
Clear flash:/b.cfg? [Y/N]:y
Clearing file flash:/b.cfg... Done.
```

関連コマンド

delete

5.1.16 rmdir

Syntax

rmdir *directory*

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: ディレクトリ名を指定します。

説明

rmdir コマンドはディレクトリを削除します。

ディレクトリを削除するため、ディレクトリのすべてのファイルとサブディレクトリを完全に削除するかごみ箱に移動する必要があります。ごみ箱に移動する場合、**rmdir** コマンドを実行して完全に削除することができます。

例

ディレクトリ subtest を削除します。

Delete the subtest directory.

<AP>rmdir subtest/

```
Remove directory flash:/test/subtest and the files in the recycle-bin under this
directory will be deleted permanently. Continue? [Y/N]:y
Removing directory flash:/test/subtest... Done.
```

5.1.17 tar create

Syntax

tar create [**gz**] *archive-file dest-file* [**verbose**] **source** { *source-file* | *source-directory* }&<1-5>

View

User view

定義済みユーザロール

network-admin

パラメータ

gz: ファイル、ディレクトリをアーカイブする前に **gzip** コマンドでファイル、ディレクトリを圧縮します。指定しない場合、圧縮しないでファイル、ディレクトリをアーカイブします。

archive-file dest-file: アーカイブファイル名を指定します。**gz** パラメータを指定する場合、引数の拡張子は“.tar.gz”にする必要があります。**gz** パラメータを指定しない場合、引数の拡張子は“.tar”にする必要があります。

verbose: 正常にアーカイブされたファイル、ディレクトリの名前を表示します。指定しない場合、ファイル、ディレクトリの名前を表示しません。

source { *source-file* | *source-directory* }&<1-5>: アーカイブされるファイル、ディレクトリを指定します。引数は半角スペースで区切ることで 5 つまで指定することができます。

説明

tar create コマンドはファイル、ディレクトリをアーカイブします。

例

ファイル 1.cfg、2.cfg、ディレクトリ test をファイル a.tar にアーカイブします。

<AP> tar create archive-file a.tar source 1.cfg 2.cfg test

```
Creating archive flash:/a.tar Done.
```

ファイル 1.cfg、2.cfg、ディレクトリ test をファイル b.tar.gz に圧縮してアーカイブします。

<AP> tar create gz archive-file b.tar.gz source 1.cfg 2.cfg test

```
Creating archive flash:/b.tar.gz Done.
```

ファイルとディレクトリを圧縮、アーカイブします。アーカイブしたファイルとディレクトリを表示します。

<AP> tar create gz archive-file c.tar.gz verbose source 1.cfg 2.cfg test

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

関連コマンド

- **tar extract**
- **tar list**

5.1.18 tar extract

Syntax

tar extract archive-file *file* [**verbose**] [**screen** | **to** *directory*]

View

User view

定義済みユーザロール

network-admin

パラメータ

archive-file *file*: アーカイブファイル名を指定します。拡張子は ".tar" あるいは ".tar.gz" です。

verbose: 正常に解凍したファイルとディレクトリの名前を表示します。

screen: 画面に解凍したファイルとディレクトリの内容を表示します。解凍したファイルは保存されません。

to *directory*: 解凍したファイルとディレクトリをパスに保存します。directory 引数はディレクトリを指定します。

説明

tar extract コマンドはファイルとディレクトリを解凍します。

screen パラメータあるいは **to** *directory-name* パラメータを指定しない場合、解凍したファイルとディレクトリを解凍し、解凍ファイルとして同一ディレクトリに保存します。

コマンドはもとの名前を使用して、解凍したファイル、ディレクトリを保存します。既に同一ファイル、ディレクトリが存在する場合、解凍したファイル、ディレクトリを既存のファイル、ディレクトリに上書きします。

screen キーワードを指定する場合は、ファイルサイズに注意してください。ファイルが大きい場合、コマンドに時間がかかることがあります。出力を停止することはできず、コンフィグレーション端末がクラッシュする可能性があります。

例

アーカイブファイル a.tar からファイル、ディレクトリを解凍します。

<AP> tar extract archive-file a.tar

```
Extracting archive flash:/a.tar Done.
```

アーカイブファイル a.tar からファイルとディレクトリを解凍し、アーカイブしたファイルとディレクトリの名前を表示します。

<AP> tar extract archive-file b.tar.gz verbose

```
1.cfg
2.cfg
```

```
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

アーカイブファイル a.tar からファイルを解凍し、アーカイブしたファイルの内容を表示します。

<AP> tar extract archive-file a.tar screen

```
#
 version 7.1.055, Demo 2501008
#
 sysname AP
#
...
```

関連コマンド

- **tar create**
- **tar list**

5.1.19 tar list

Syntax

tar list archive-file *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

archive-file *file*: アーカイブファイル名を指定します。拡張子は “.tar” あるいは “.tar.gz” です。

説明

tar list コマンドはアーカイブしたファイルとディレクトリの名前を表示します。

例

アーカイブしたファイルとディレクトリの名前を表示します。

<AP> tar list archive-file a.tar

```
1.cfg
2.cfg
test/
test/a.log
test/subtest/
test/subtest/aa.log
```

関連コマンド

- **tar create**
- **tar extract**

5.1.20 undelete

Syntax

undelete *file*

View

User view

定義済みユーザロール

network-admin

パラメータ

file: 復元するファイルの名前を指定します。

説明

undelete コマンドはごみ箱からファイルを復元します。

ディレクトリに同一名のファイルが存在する場合、既存のファイルに上書きするかどうかの画面を表示します。”Y”を入力した場合、既存のファイルは上書きされます。”N”を入力した場合、このコマンドは実行されません。

例

copy.cfg ファイルを復元します。このファイルはディレクトリ flash:からごみ箱に移動されたファイルです。

<AP> undelete copy.cfg

```
Undelete flash:/copy.cfg? [Y/N]:y
Undeleting file flash:/copy.cfg... Done.
```

ファイル startup.cfg を復元します。このファイルはディレクトリ flash:/seclog からごみ箱に移動されたファイルです。

- 方法 1:

<AP> undelete seclog/startup.cfg

```
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
```

<AP>

- 方法 2:

<AP> cd seclog

<AP> undelete startup.cfg

```
Undelete flash:/seclog/startup.cfg? [Y/N]:y
Undeleting file flash:/seclog/startup.cfg... Done.
```

目次

このセクションのページは **1-x-x** です。

6 章 コンフィグレーションファイル管理 6-1
6.1 コンフィグレーションファイル管理設定コマンド 6-1
6.1.1 backup startup-configuration 6-1
6.1.2 display current-configuration 6-2
6.1.3 display current-configuration diff 6-4
6.1.4 display default-configuration 6-7
6.1.5 display diff 6-8
6.1.6 display saved-configuration 6-11
6.1.7 display startup 6-13
6.1.8 display this 6-14
6.1.9 reset saved-configuration 6-16
6.1.10 restore startup-configuration 6-18
6.1.11 save 6-20
6.1.12 startup saved-configuration 6-22

6章 コンフィグレーションファイル管理

6.1 コンフィグレーションファイル管理設定コマンド

6.1.1 backup startup-configuration

Syntax

backup startup-configuration to *ipv4-server* [*dest-filename*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv4-server: IPv4 アドレスあるいはホスト名で TFTP サーバを指定します。ホスト名は大文字小文字を区別しない 1～253 文字の文字列です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

dest-filename: サーバの次回起動時に使用する起動コンフィグレーションファイルを保存するためのターゲットファイル名を指定します。ファイル名の拡張子は”.cfg”です。ターゲットファイル名を指定しない場合、ソースファイル名が使用されます。

説明

backup startup-configuration コマンドは TFTP サーバに次回の起動に使用する起動コンフィグレーションファイルをバックアップします。

例

TFTP サーバ 2.2.2.2 に次回の起動に使用する起動コンフィグレーションファイル 192-168-1-26.cfg をバックアップします。

<AP> backup startup-configuration to 2.2.2.2 192-168-1-26.cfg

```
Backing up the main startup configuration file to 2.2.2.2...
```

関連コマンド

restore startup-configuration

6.1.2 display current-configuration

Syntax

display current-configuration [**configuration** [*module-name*] |**exclude-provision** | **interface** [*interface-type* [*interface-number*]]] [**by-section** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

configuration [*module-name*]: 機能の設定を表示します。*module-name* 引数は機能モジュールを指定します。指定されない場合、設定されたすべての機能を表示します。有効な機能モジュールは装置の設定に依存します。

exclude-provision: 事前にプロビジョニングされた設定を running configuration から除外します。

interface [*interface-type* [*interface-number*]]: インタフェースの設定を表示します。*interface-type* 引数はインタフェースタイプで、*interface-number* 引数はインタフェース番号を示します。

by-section: running configuration をセクション別に表示します。各セクションには command view のコンフィグが含まれており、隣接する 2 つのセクションはポンド記号 (#) で区切られています。このキーワードを指定しない場合、コマンドは running configuration を行ごとに表示します。

begin: 指定した正規表現に一致する最初のコンフィグセクションと、後続のすべてのコンフィグセクションを表示します。

exclude: 指定した正規表現に一致しないすべてのコンフィグセクションを表示します。

include: 指定された正規表現に一致するすべてのコンフィグセクションを表示します。

正規表現: コンフィグセクションをフィルタリングするための正規表現を指定します。大文字と小文字が区別される 1 ～ 256 文字の文字列です。

指定された正規表現に一致するコマンドラインがセクションに含まれている場合、そのセクションは指定された正規表現に一致します。

説明

display current-configuration コマンドは現在の有効な設定を表示します。

本コマンドを使用して設定の確認を行うことができます。

システムは自動的にパラメータの設定を変更します。たとえば、システムの制限に合わない設定がある場合、自動的に変更します。設定が変更されると、システムの制限に適合した設定を表示します。

デフォルトの設定を使用しないパラメータは表示されません。

例

ローカルユーザの設定を表示します。

<AP> display current-configuration configuration local-user

```
#
local-user ftp
 password                                                                hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfD
If8ROLtVErJ/C31oq2rFtmNuyZf4STw==
 service-type ftp
 authorization-attribute user-role network-operator
#
local-user root
 password                                                                hash
$h$6$Twd73mLrN8O2vvD5$Cz1vgdpR4KoTiRQNE9pg33gU14Br2p1VguczLSVyJLO2huV5Syx/LfD
If8ROLtVErJ/C31oq2rFtmNuyZf4STw==
 service-type ssh telnet terminal
 authorization-attribute user-role network-admin
#
return
```

6.1.3 display current-configuration diff

Syntax

display current-configuration diff

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display current-configuration diff コマンドは現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイル間のコンフィグレーション差分を表示します。

本コマンドは、以下のステップで現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイルを比較します。

1) 現在のコンフィグレーションファイルと、次回の起動に使用するメインのコンフィグレーションファイルを比較します。
2) 次回の起動に使用するメインのコンフィグレーションファイルが利用不可または壊れている場合は、本コマンドはバックアップの次回の起動に使用するコンフィグレーションファイルと現在のコンフィグレーションファイルを比較します。

メインとバックアップの両方の次回の起動に使用するコンフィグレーションファイルが利用不可または壊れている場合は、システムは、次回の起動に使用するコンフィグレーションファイルが存在しないことを示すメッセージを表示します。

例

現在のコンフィグレーションファイルと次回の起動に使用するコンフィグレーションファイル間のコンフィグレーション差分を表示します。

<AP> display current-configuration diff

```
--- Startup configuration
+++ Current configuration
@@ -17,7 +17,9 @@
 #
 vlan 200
 #
-vlan 300
+vlan 400
+#
+vlan 500
```

```
 #
<AP>
```

表 6-1 コマンド出力

フィールド	説明
- - - A +++ B	● **A**ー比較元のコンフィグレーションファイルを表示します。**Startup configuration**、**Current configuration**、ディレクトリ情報を含む比較元設定ファイル名のいずれかを示します。 ● **B**ー比較対象のコンフィグレーションファイルを表示します。**Current configuration**、**Startup configuration**、ディレクトリ情報を含む比較対象設定ファイル名のいずれかを示します。 ● この例では**Startup configuration**、**Current configuration**はそれぞれ比較元のコンフィグレーションファイル、比較先コンフィグレーションファイルです。
@@ *-linenumber1,number1* *+linenumber2,number2* @@	コマンドラインの相違に関する位置の概要です。 ● *-linenumber1,number1*—相違が含まれる比較元の設定です。*linenumber1*はセクションの開始行を示します。*nunber1*のセクションの開始行と最終行間での行の数を示します。 ● *+linenumber2,number2*—相違が含まれる比較先の設定です。*linenumber2*はセクションの開始行を示します。*nunber2*のセクションの開始行と最終行間での行の数を示します。

フィールド	説明
cmd1 - cmd2 + cmd3 cmd4	比較したコンフィグレーションファイルの相違を示します。 ● *cmd1*、*cmd4*ーコマンドラインの先頭に（-）あるいは（+）がついていない場合、比較元と比較先のコンフィグレーションファイルの両方のコマンドラインの行が含まれます。これはコマンドラインの相違の位置を示すための情報です。 ● *-cmd2*ーコマンドラインに比較元のコンフィグレーションファイルに記載されているが、比較先のコンフィグレーションファイルに記載されていない場合、（-）の記号がコマンドラインの先頭に表示されます。 ● *-cmd3*ーコマンドラインに比較先のコンフィグレーションファイルに記載されているが、比較元のコンフィグレーションファイルに記載されていない場合、（+）の記号がコマンドラインの先頭に表示されます。 ● この例ではVLAN 200、Vlan-interface1が両方のコンフィグレーションファイルに含まれていることを示します。VLAN 400、VLAN 500は**Current configuration**にのみ含まれています。VLAN 300は**Startup configuration**にのみ含まれています。

関連コマンド

- **display current-configuration**
- **display diff**
- **display saved-configuration**

6.1.4 display default-configuration

Syntax

display default-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display default-configuration コマンドは工場出荷状態のデフォルトコンフィグレーション設定を表示します。

工場出荷状態のコンフィグレーションはデフォルトコンフィグレーションファイルにあります。製品仕様のデフォルト設定は初期設定と異なります。設定ファイルがない場合あるいは設定ファイルが壊れている場合、デフォルト設定によって装置が起動し、正常に動作するようにします。

例

デフォルトコンフィグレーション設定を表示します。

<AP> display default-configuration

6.1.5 display diff

Syntax

display diff configfile *file-name-s* { **configfile** *file-name-d* | **current-configuration** | **startup-configuration** }

display diff current-configuration { **configfile** *file-name-d* | **startup-configuration** }

display diff startup-configuration { **configfile** *file-name-d* | **current-configuration** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

configfile *file-name-s*: 比較元のコンフィグレーションファイルを指定します。

configfile *file-name-d*: 比較先のコンフィグレーションファイルを指定します。

current-configuration: 現在のコンフィグレーションファイルを指定します。**display diff current-configuration** コマンドにおいて、このパラメータは、比較元のコンフィグレーションファイルを指定します。他の 2 つの **display diff** コマンドにおいて、このパラメータは比較先のコンフィグレーションファイルを指定します。

startup-configuration: 次回の起動に使用するコンフィグレーションを指定します。**display diff startup-configuration** コマンドにおいて、このパラメータは比較元のコンフィグレーションを指定します。他の 2 つの **display diff** コマンドにおいて、このパラメータは比較先のコンフィグレーションを指定します。

説明

display diff コマンドはコンフィグレーション差分を表示します。

startup-configuration キーワードを指定した場合、システムは次回の起動に使用するメインのコンフィグレーションを比較するために、以下の順序で検索します。

1) 次回の起動に使用するメインのコンフィグレーションファイル
2) 次回の起動に使用するメインのコンフィグレーションファイルが利用不可な場合は、本コマンドはバックアップの次回の起動に使用するコンフィグレーションファイル

メインとバックアップの両方の次回の起動に使用するコンフィグレーションファイルが利用不可な場合は、システムは、次回の起動に使用するコンフィグレーションファイルが存在しないことを示すメッセージを表示します。

例

startup.cfg と test.cfg のコンフィグレーション差分を表示します。

<AP> display diff configfile startup.cfg configfile test.cfg

```
--- flash:/startup.cfg
+++ flash:/test.cfg
@@ -17,7 +17,9 @@
 #
 vlan 200
 #
-vlan 300
+vlan 400
+#
+vlan 500
 #
 interface Vlan-interface1
 #
```

<AP>

出力では、VLAN200 と VLAN-interface 1 は両方のコンフィグレーションに含まれています。は VLAN 400、VLAN 500 は test.cfg のみに含まれますが、VLAN 300 は startup.cfg のみに含まれます。

<AP> display diff current-configuration startup-configuration

```
--- Current configuration
+++ Startup configuration
@@ -17,9 +17,7 @@
 #
 vlan 200
 #
-vlan 400
--#
--vlan 500
+vlan 300
 #
 interface Vlan-interface1
 #
```

<AP>

出力では、VLAN 200 と VLAN-interface 1 は両方のコンフィグレーションに含まれています。は VLAN 400、VLAN 500 は test.cfg のみに含まれますが、VLAN 300 は startup.cfg のみに含まれます。

出力の詳細は表 6-3 を参照してください。

関連コマンド

- **display current-configuration**
- **display current-configuration diff**

- **display saved-configuration**

6.1.6 display saved-configuration

Syntax

display saved-configuration [**by-section** { **begin** | **exclude** | **include** }

regular-expression]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

by-section: 次回起動時のコンフィグをセクション別に表示します。各セクションには command view に設定が含まれており、隣接する 2 つのセクションはポンド記号 (#) で区切られています。このキーワードを指定しない場合、コマンドは次の始動時に使用されるコンフィグを行ごとに表示します。

begin: 指定した正規表現に一致する最初のコンフィグセクションと、後続のすべてのコンフィグセクションを表示します。

exclude: 指定した正規表現に一致しないすべてのコンフィグセクションを表示します。

include: 指定された正規表現に一致するすべてのコンフィグセクションを表示します。

regular-expression: コンフィグセクションをフィルタリングするための正規表現を指定します。大文字と小文字が区別される 1 ～ 256 文字の文字列です。指定された正規表現に一致するコマンド ラインがセクションに含まれている場合、そのセクションは指定された正規表現に一致します。

説明

display saved-configuration コマンドは装置が次回に起動に使用するために保存されているコンフィグレーションファイルの内容を表示します。

本コマンドは、装置の次回に起動するときに使用できるように重要な設定がコンフィグレーションファイルに保存されているかどうかを確認することができます。

以下の順番でコンフィグレーションファイルを選択します。

1) メインのコンフィグレーションファイルが有効である場合、メインのコンフィグレーションファイルの内容を表示します。
2) バックアップのコンフィグレーションファイルが有効である場合、バックアップのコンフィグレーションファイルの内容を表示します。
3) メインのコンフィグレーションファイルとバックアップのコンフィグレーションファイルが有効でない場合、何も表示されません。

例

次回に起動するコンフィグレーションファイルの内容を表示します。

<AP> display saved-configuration

```
#
 version 7.1.1
#
 sysname AP
#
 undo copyright-info enable
#
 undo info-center logfile enable
#
 undo lldp global enable#
#
vlan 1
#
  ---- More ----
```

関連コマンド

- **reset saved-configuration**
- **save**

6.1.7 display startup

Syntax

display startup

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display startup コマンドは現在のスタートアップコンフィグレーションファイルと次回に起動するコンフィグレーションファイルの名前を表示します。

例

スタートアップコンフィグレーションファイルの名前を表示します。

<AP> display startup

```
Current startup saved-configuration file: flash:/startup.cfg
Next main startup saved-configuration file: flash:/startup.cfg
Next backup startup saved-configuration file: NULL
```

表 6-2 コマンド出力

フィールド	説明
Current startup saved-configuration file	装置が起動した際のコンフィグレーションファイルです。
Next main startup saved-configuration file	次回起動する際に使用するメインコンフィグレーションファイルです。
Next backup startup saved-configuration file	次回起動する際に使用するバックアップコンフィグレーションファイルです。

関連コマンド

startup saved-configuration

6.1.8 display this

Syntax

display this [**by-section** { **begin** | **exclude** | **include** } regular-expression]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

by-section: 現在のビューの running configuration をセクション別に表示します。各セクションには command view に設定が含まれており、隣接する 2 つのセクションはポンド記号 (#) で区切られています。このキーワードを指定しない場合、コマンドは running configuration を現在のビューに行ごとに表示します。

begin: 指定した正規表現に一致する最初のコンフィグセクションと、後続のすべてのコンフィグセクションを表示します。

exclude: 指定した正規表現に一致しないすべてのコンフィグセクションを表示します。

include: 指定された正規表現に一致するすべてのコンフィグセクションを表示します。

regular-expression: コンフィグセクションをフィルタリングするための正規表現を指定します。大文字と小文字が区別される 1 ～ 256 文字の文字列です。指定された正規表現に一致するコマンド ラインがセクションに含まれている場合、そのセクションは指定された正規表現に一致します。

説明

display this コマンドは現在の view の有効な設定を表示します。

現在の view で行った設定を確認するために使用します。

このコマンドはデフォルト設定のパラメータは表示されません。

パラメータに関する機能が無効であったとしても、パラメータを設定することができます。これらのパラメータは機能が有効になったのち、表示されます。

すべての line view でこのコマンドを使用すると、すべてのラインインタフェースで有効な設定情報を表示します。

例

インタフェース GigabitEthernet1/0/1 で有効な設定を表示します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
 port-isolate enable
#
return
```

ユーザ line で有効な設定を表示します。

<AP> system-view

[AP] line vty 0

[AP-line-vty0] display this

```
#
line con 0
 user-role network-admin
#
line vty 0 63
 authentication-mode none
 user-role network-admin
#
return
```

6.1.9 reset saved-configuration

Syntax

reset saved-configuration [**backup** | **main**]

View

User view

定義済みユーザロール

network-admin

パラメータ

backup: バックアップの次回の起動時に使用するコンフィグレーションファイルを削除します。

main: メインの次回の起動時に使用するコンフィグレーションファイルを削除します。

説明

reset saved-configuration コマンドは次回の起動時に使用するコンフィグレーションファイルを削除します。

⚠ **注意:**

本コマンドの使用にあたっては注意してください。本コマンドは次回の起動時に使用するコンフィグレーションファイルを削除します。

ソフトウェアバージョンが一致していない、あるいはコンフィグレーションファイルが壊れている場合、次回の起動時に使用するコンフィグレーションファイルを削除します。

メイン、バックアップ、あるいは両方の次回の起動時に使用するコンフィグレーションファイルを削除することができます。

メインとバックアップの次回の起動時に使用するコンフィグレーションファイルを削除するため、**reset saved-configuration backup** コマンドと **reset saved-configuration main** コマンドの両方を実行する必要があります。コマンドの一方を削除することで、ファイルの削除の代わりに指定したファイルの属性を削除することができます。

たとえば、**reset saved-configuration backup** コマンドが実行されるとバックアップの次回の起動時に使用するコンフィグレーションファイルは NULL に設定されます。しかしファイルはメインファイルとして使用されます。ファイルを削除するために、**reset saved-configuration main** コマンドを実行する必要があります。

コンフィグレーションファイルの属性が指定されていない場合、**reset saved-configuration** コマンドはメインの次回の起動時に使用するコンフィグレーションファイルを削除します。

例

メインの次回の起動時に使用するコンフィグレーションファイルを削除します。

<AP> reset saved-configuration

```
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in flash: is being cleared.
Please wait ...........
Configuration file is cleared.
```

関連コマンド

display saved-configuration

6.1.10 restore startup-configuration

Syntax

restore startup-configuration from *ipv4-server src-filename*

View

User view

定義済みユーザロール

network-admin

パラメータ

ipv4-server: IPv4 アドレスあるいはホスト名で TFTP サーバを指定します。ホスト名は大文字小文字を区別しない 1～253 文字の文字列です。大文字、小文字を区別しません。ホスト名で使用できる文字列は文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

src-filename: 拡張子が“.cfg”の、ダウンロードされたコンフィグレーションファイルのファイル名を指定します。拡張子を除くファイル名は大文字小文字を区別しない 1～255 文字の文字列です。

説明

restore startup-configuration コマンドは指定した TFTP サーバからコンフィグレーションファイルをダウンロードし、次回の起動時に使用するメインのコンフィグレーションファイルとして指定します。

次回の起動時に使用するコンフィグレーションファイルを指定する前に、以下の要件を確認してください。

- サーバへ到達可能であること。
- サーバが TFTP サービスを有効にしています。
- サーバへの読み込み、書き込み許可があります。

本コマンドは、メインの次回の起動時に使用するコンフィグレーションファイルの復旧を自動で行うことで、コンフィグレーションファイルの復旧を簡単に行うことができます。

例

TFTP サーバ 2.2.2.2 からコンフィグレーションファイル **test.cfg** をダウンロードし、次回の起動時に使用するコンフィグレーションファイルとして指定します。

<AP> restore startup-configuration from 2.2.2.2 test.cfg

```
Restoring the next startup-configuration file from 2.2.2.2...
Done.
```

関連コマンド

backup startup-configuration

6.1.11 save

Syntax

save *file-url*

save [**safely**] [**backup** | **main**] [**force**] [**changed**]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

file-url: 動作中のコンフィグレーションを指定されたファイルに“.cfg”拡張子で、ファイルを次回起動時のコンフィグレーションファイルとして指定せずに保存します。“.cfg”拡張子を除き、ファイル名は大文字小文字を区別しない 1～255 文字の文字列で、パス情報を含むことができます。有効な文字は、文字、数字、ハイフン（-）、アンダーライン（-）、ドット（.）です。

safely: safe モードでコンフィグレーションファイルを保存します。このパラメータを指定しない場合、装置は fast モードでコンフィグレーションファイルを保存します。safe モードは fast モードよりも保存に要する時間が遅くなりますが、安全に行うことができます。

backup: 動作中のコンフィグレーションを指定したファイルに保存し、バックアップの次回に起動するコンフィグレーションファイルとして指定します。**backup** パラメータあるいは **main** パラメータを指定しない場合、保存したファイルをメインの次回に起動するコンフィグレーションファイルに指定します。

main: 動作中のコンフィグレーションを指定したファイルに保存し、メインの次回に起動するコンフィグレーションファイルとして指定します。**main** パラメータあるいは **backup** パラメータを指定しない場合、保存したファイルをメインの次回に起動するコンフィグレーションファイルに指定します。

force: 動作中のコンフィグレーションを、確認の表示を行わずに保存します。本パラメータを指定しない場合、操作を実行する際に確認メッセージが表示されます。30 秒以内に操作を行わない場合、システムは自動で操作を中止します。30 秒以内に"Y"を入力すると、保存処理を継続し、処理中のターゲットファイル名を変更することができます。

changed: コンフィギュレーション ファイルと running configuration の設定に矛盾が検出された場合、ターゲット コンフィギュレーション ファイルを running configuration で上書きします。不整合が検出されない場合、save コマンドは適用しません。このキーワードを指定しない場合、save コマンドは常にターゲット コンフィギュレーション ファイルを running configuration 上書きします。

説明

save *file-url* [**all**]コマンドは動作中のコンフィグレーションをコンフィグレーションファイルに保存します。次回に起動するコンフィグレーションファイルとして指定しません。

save [**safely**] [**backup** | **main**] [**force**]コマンドは記憶媒体のルートディレクトリのファイルに動作中のコンフィグレーションを保存します。本コマンドは次回に起動するコンフィグレーションファイルとして自動的に指定します。

本コマンドで指定されたファイルが存在しない場合、設定を保存する前、システムはファイルを作成します。すでにファイルが存在する場合、システムはファイルを上書きするかどうか確認メッセージを表示します。ファイルを上書きしない場合、システムは**save** コマンドの操作を中止します。

コマンドの *file-url* パラメータを指定しない場合、コマンドはテキストファイル”.cfg”と、バイナリファイル”.mdb”に動作中のコンフィグレーションを保存します。2 つのファイルは同一ファイル名です。バイナリファイル”.mdb”はテキストファイル”.cfg”よりも保存に要する時間が短くなります。

safe モードでは、システムは一時ファイルに設定を保存し、保存が完了した後、ターゲットの次回の起動に使用するコンフィグレーションファイルの上書きを開始します。動作に、再起動、電源の故障あるいはメモリ容量の不足が発生した場合、次回の起動に使用するコンフィグレーションファイルは保持されています。

fast モードでは、装置は直接ターゲットの次回の起動に使用するコンフィグレーションファイルを上書きします。動作中に、再起動、電源の故障あるいはメモリ容量の不足が発生した場合、次回の起動に使用するコンフィグレーションファイルが消失します。

例

動作中のコンフィグレーションをコンフィグレーションファイル backup.cfg に保存し、次回に起動するコンフィグレーションファイルとして指定しません。

<AP> save backup.cfg

```
The current configuration will be saved to flash:/backup.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration
flash:/backup.cfg. Please wait...
Configuration is saved to successfully.
```

動作中のコンフィグレーションをメインの次回の起動に使用するコンフィグレーションファイルに、確認の表示を行わずに保存します。

<AP> save force

```
Validating file. Please wait....
Saved the current configuration to mainboard device successfully.
```

動作中のコンフィグレーションを記憶媒体のルートディレクトリのファイルに保存し、メインの次回の起動に使用するコンフィグレーションファイルとして指定します。

<AP> save

```
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/backup.cfg]
(To leave the existing filename unchanged, press the enter key):test.cfg
 Validating file. Please wait.....
 Configuration is saved to device successfully.
```

関連コマンド

- **display current-configuration**
- **display saved-configuration**

6.1.12 startup saved-configuration

Syntax

startup saved-configuration *cfgfile* [**backup** | **main**]

undo startup saved-configuration

デフォルト

次回の起動に使用するコンフィグレーションファイルは指定されていません。

View

User view

定義済みユーザロール

network-admin

パラメータ

cfgfile: “.cfg”拡張子をつけてコンフィグレーションファイル名を指定します。“.cfg”拡張子を除き、ファイル名は大文字小文字を区別しない 1～255 文字の文字列で、パス情報を含むことができます。有効な文字は、文字、数字、ハイフン(-)、アンダーライン(-)、ドット（.）です。ファイルパスがディレクトリ名を含む場合は、ディレクトリが既に存在している必要があります。

backup: コンフィグレーションファイルをバックアップの次回の起動に使用するコンフィグレーションファイルとして指定します。

main: コンフィグレーションファイルをメインの次回の起動に使用するコンフィグレーションファイルとして指定します。これは、装置が起動時に読み込みを行うメインのコンフィグレーションファイルです。読み込みに失敗した場合、装置はバックアップの次回の起動に使用するコンフィグレーションファイルの読み込みを行います。

説明

startup saved-configuration コマンドはファイルを次回の起動に使用するコンフィグレーションファイルとして指定します。

undo startup saved-configuration コマンドは次回の起動時に工場出荷状態で起動します。

backup パラメータあるいは **main** パラメータの両方とも指定されていない場合、**startup saved-configuration** コマンドはメインの次回の起動に使用するコンフィグレーションファイルとして指定します。

メインとバックアップのコンフィグレーションファイルを同一にすることができますが、高可用性のために、別々のファイル名としてファイルを指定することを推奨します。

undo startup saved-configuration コマンドはメインとバックアップの次回の起動に使用するコンフィグレーションファイルの属性を NULL に変更しますが、コンフィグレーションファイルを削除しません。

save コマンドで動作中のコンフィグレーションを保存したとき、次回の起動に使用するコンフィグレーションファイルとして設定することができます。

例

メインの次回の起動に使用するコンフィグレーションファイルを指定します。

<AP> startup saved-configuration testcfg.cfg

```
Please wait ....
... Done!
```

関連コマンド

display startup

目次

このセクションのページは **1-x-x** です。

7 章 ソフトウェアアップグレード 7-1
7.1 ソフトウェアアップグレードコマンド 7-1
7.1.1 boot-loader file 7-1
7.1.2 display boot-loader 7-4

7章 ソフトウェアアップグレード

7.1 ソフトウェアアップグレードコマンド

7.1.1 boot-loader file

Syntax

boot-loader file boot *filename* **system** *filename* [**feature** *filename*] { **backup** | **main** }

boot-loader file *ipe-filename* { **backup** | **main** }

View

User view

定義済みユーザロール

network-admin

パラメータ

boot: ブートイメージファイルを指定します。

system: システムイメージファイルを指定します。

feature: 最大 30 個の機能イメージファイルのスペース区切りのリストを指定します。

filename: .bin ファイルを *filesystemname/filename.bin* の形式で指定します。このファイルは、装置上のファイルシステムのルートディレクトリに格納する必要があります。ファイルシステムの場所セクション (存在する場合) を除くと、値の文字列は最大 63 文字です。ファイルシステムの詳細については、コマンドマニュアルのセクション 1 *基本機能 "ファイルシステム管理"* を参照してください。

ipe-filename: .ipe イメージパッケージファイルを *filesystemname/filename.ipe* 形式で指定します。このファイルは、装置上のファイルシステムのルートディレクトリに格納する必要があります。ファイルシステムの場所セクション (存在する場合) を除くと、値の文字列は最大 63 文字です。ファイルシステムの詳細については、コマンドマニュアルのセクション 1 *基本機能 "ファイルシステム管理"* を参照してください。

backup: バックアップ起動イメージファイルとしてファイルを指定します。バックアップイメージは、メインイメージが使用できない場合にのみ使用されます。

main: メイン起動イメージファイルとしてファイルを指定します。装置は常にメイン起動イメージファイルから起動を試みます。

説明

boot-loader file コマンドは、スタートアップイメージファイルを指定します。

boot-loader file コマンドは、スタートアップイメージリスト全体を上書きします。新しいスタートアップ機能イメージを追加するには、機能イメージファイルを含む、古いスタートアップイメージリスト内のすべての機能イメージファイルを指定します。新しいスタートアップイメージリストには、コマンドで指定された機能イメージファイルのみが含まれます。

指定したスタートアップソフトウェアイメージをロードするには、システムを再起動する必要があります。

boot-loader file コマンドを使用してインクリメンタルパッチをインストールすることはできません。

装置が展開された.bin ファイルのロードに失敗した場合、バックアップ起動イメージファイルがロードされます。

🕮 **メモ：**

システムは、指定されたイメージでスタートアップイメージリストを更新する前に、指定されたイメージのデジタル署名を検証します。デジタル署名検証が失敗した場合、システムはスタートアップイメージリストを更新せず、デジタル署名検証失敗メッセージが表示されます。

例

メイン起動イメージファイルとして **flash:/qx-w610.ipe** を指定します。

<AP> boot-loader file flash:/qx-w610.ipe main

```
QX-W610 images in IPE:
  qx-w610-boot-v7595.bin
  qx-w610-system-v7595.bin
  qx-w610-freeradius-v7595.bin
This command will set the main startup software images. Please do not reboot the
device during the upgrade. Continue? [Y/N]:y
Add images to the device.
File flash:/qx-w610-boot-v7595.bin already exists on the device.
File flash:/qx-w610-system-v7595.bin already exists on the device.
File flash:/qx-w610-freeradius-v7595.bin already exists on the device.
Overwrite the existing files?[Y/N]:y
Decompressing            file            qx-w610-boot-v7595.bin            to
flash:/qx-w610-boot-v7595.bin....Done.
Decompressing           file           qx-w610-system-v7595.bin           to
flash:/qx-w610-system-v7595.bin.....................Done.
Decompressing          file          qx-w610-freeradius-v7595.bin          to
flash:/qx-w610-freeradius-v7595.bin.......Done.
Verifying the file flash:/qx-w610-boot-v7595.bin on the device...Done.
Verifying the file flash:/qx-w610-system-v7595.bin on the device..........Done.
Verifying the file flash:/qx-w610-freeradius-v7595.bin on the device....Done.
```

```
The images that have passed all examinations will be used as the main startup
software images at the next reboot on the device.
Decompression completed.
You are recommended to delete the .ipe file after you set startup software images
for all slots.
Do you want to delete flash:/qx-w610.ipe now? [Y/N]:y
```

#メインスタートアップブートおよびシステムイメージファイルとして flash:/boot.bin および flash:/system.bin を指定します。

<AP>boot-loader file boot flash:/boot.bin system flash:/system.bin main

```
This command will set the main startup software images. Continue? [Y/N]:Y
The images that have passed all examinations will be used as the main startup
software images at the next reboot on the device.
```

関連コマンド

display boot-loader

7.1.2 display boot-loader

Syntax

display boot-loader

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display boot-loader コマンドは現在のソフトウェアイメージと起動ソフトウェアイメージが表示されます。

例

現在のソフトウェアイメージと起動ソフトウェアイメージを表示します。

<AP> display boot-loader

```
Software images on the device:
Current software images:
  Image                                          Version
  flash:/qx-w610-boot-v7595.bin                   7.5.95
  flash:/qx-w610-system-v7595.bin                 7.5.95
  flash:/qx-w610-freeradius-v7595.bin             7.5.95
Main startup software images:
  Image                                          Version
  flash:/qx-w610-boot-v7595.bin                   7.5.95
  flash:/qx-w610-system-v7595.bin                 7.5.95
  flash:/qx-w610-freeradius-v7595.bin              7.5.95
Backup startup software images:
  None
```

表 7-1 コマンド出力

フィールド	説明
Current software images	起動時にロードされたComwareイメージ。
Main startup software images	次の起動時に使用するComwareイメージ。
Image	Comwareイメージのファイル名。

フィールド	説明
Version	イメージバージョン。 イメージが破損または削除された場合、このフィールドには2つのハイフン(--)が表示されます。
Backup startup software images	次の起動時に使用するバックアップComwareイメージ。 バックアップ起動ソフトウェアイメージが指定されていない場合、このフィールドには**None**と表示されます。

関連コマンド

- **boot-loader file**

QX-W610 アクセスポイント

コマンドマニュアル

02. システム管理

本マニュアルは以下に示す章で構成されています。

01-装置管理

02-NTP

03-Information Center

目次

このセクションのページは **2-x-x** です。

1 章 装置管理 1-1
1.1 装置管理コマンド 1-1
1.1.1 clock datetime 1-1
1.1.2 clock protocol 1-3
1.1.3 clock summer-time 1-4
1.1.4 clock timezone 1-6
1.1.5 command 1-8
1.1.6 copyright-info enable 1-10
1.1.7 diag boot-info display 1-10
1.1.8 display clock 1-14
1.1.9 display copyright 1-15
1.1.10 display cpu-usage 1-16
1.1.11 display cpu-usage history 1-17
1.1.12 display device 1-20
1.1.13 display device manuinfo 1-21
1.1.14 display diagnostic-information 1-22
1.1.15 display memory 1-23
1.1.16 display memory-threshold 1-25
1.1.17 display scheduler job 1-26
1.1.18 display scheduler logfile 1-28
1.1.19 display scheduler reboot 1-29
1.1.20 display version 1-29
1.1.21 header 1-32
1.1.22 job 1-34
1.1.23 memory-threshold 1-35
1.1.24 monitor cpu-usage enable 1-36
1.1.25 monitor cpu-usage interval 1-38
1.1.26 monitor cpu-usage threshold 1-39
1.1.27 password-recovery enable 1-40
1.1.28 reboot 1-42
1.1.29 reset scheduler logfile 1-44
1.1.30 restore factory-default 1-44
1.1.31 scheduler job 1-45
1.1.32 scheduler logfile size 1-46
1.1.33 scheduler reboot at 1-47
1.1.34 scheduler reboot delay 1-49

1.1.35 scheduler schedule 1-51
1.1.36 shutdown-interval 1-53
1.1.37 sysid 1-54
1.1.38 sysname 1-55
1.1.39 time at 1-56
1.1.40 time once 1-57
1.1.41 time repeating 1-59
1.1.42 user-role 1-61

1章 装置管理

1.1 装置管理コマンド

1.1.1 clock datetime

Syntax

clock datetime *time date*

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 時刻を指定します。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 (時) です。*mm* の設定範囲は 0～59 (分) です。*ss* の設定範囲は 0～59 (秒) です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合は、*hh* に 8 を指定することで、設定することができます。

date: 現在の日付を指定します。形式は *MM/DD/YYYY* あるいは *YYYY/MM/DD* です。*YYYY* は 2000～2035 (年) を指定することができます。*MM* は 1～12 (月)を指定することができます。*DD* は各月の日付を指定することができます。

説明

clock datetime コマンドは装置の現在の日時を設定します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

装置は、以下のタイミングでシステム時間を FLASH に書き込みます。

- reboot コマンドにより装置を再起動する前
- 装置の稼働時間が 12 時間経過する毎

装置を、ローカルシステム時間または NTP 時間ソースを使用するように設定可能です。

装置がローカルシステム時間を使用する場合、装置のシステム時間は以下の要素に依存します。

- ローカルタイムゾーン
- UTC 時間
- サマータイム

システム時間を確認するには、**display clock** コマンドを使用します。

注意:

このコマンドは、デバイスのシステム時刻を変更するコマンドです。これは、システム時刻関連機能(たとえば、スケジュールされたタスク)の実行や他の機器との共同操作機能(ログのレポートや統計情報の収集)に影響します。
このコマンドを実行する前に、運用中のネットワークへの影響を確認してください。

例

装置の現在の日時を UTC 時間で 2023/12/24 08:08:08 に設定します。

<AP> clock datetime 8:8:8 12/24/2023

装置の現在の日時を UTC 時間で 2023/12/24 08:10:00 に設定します。

<AP> clock datetime 8:10 2023/12/24

関連コマンド

- **clock protocol**
- **clock summer-time**
- **clock timezone**
- **display clock**

1.1.2 clock protocol

Syntax

clock protocol { **none** | **ntp** }

undo clock protocol

デフォルト

NTP

View

System view

定義済みユーザロール

network-admin

パラメータ

none:ローカルシステム時間です。

ntp: UTC 時間を含む NTP です。正しい NTP を設定してください。NTP の詳細はオペレーションマニュアルのセクション 2 *システム管理 "NTP"* を参照してください。

説明

clock protocol コマンドはシステムクロックソースを指定します。

undo clock protocol コマンドはデフォルトに戻します。

正しいシステム時間はネットワーク管理やネットワーク通信に必須です。ネットワーク装置を動作させる前に、システム時間を設定します。装置はローカルに設定されたシステム時間を使うか、UTC 時間をネットワークの上の時間ソースから得て、システム時間を計算することができます。

- **clock protocol none** コマンドを使用する場合、装置はローカルシステム時間を設定します。装置はその時、システム時間を維持するためにその内蔵の水晶発振器によって生成されたクロック信号を使います。
- **clock protocol ntp** コマンドを使用する場合、装置は NTP によって UTC 時間を得て、システム時間を計算します。装置は周期に UTC 時間を同期させて、システム時間を再計算します。

NTP 時間ソースから UTC 時間を使って計算されたシステム時間はより精密です。

コマンドを複数回実行した場合、最新の設定が有効になります。

例

ローカルシステム時間を使用するように設定します。

<AP> system-view

[AP] clock protocol none

1.1.3 clock summer-time

Syntax

clock summer-time *name start-time start-date end-time end-date add-time*

undo clock summer-time

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

name: サマータイム名を指定します。設定範囲は大文字小文字を区別する 1～32 文字です。

start-time: 開始時刻を指定します。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

start-date: 開始日を以下の形式の 1 つで指定します。

- *MM*/*DD*：*MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。
- *month week date*
  - **month**−月を指定します。January、February、March、April、May、June、July、August、September、October、November、December が指定できます。
  - **week**−月で開始する週を指定します。first、second、third、fourth、fifth、last が指定できます。
  - **day**−日を指定します。Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday が指定できます。

end-time: 終了時刻を指定します。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

end-date: 終了日を以下の形式の 1 つで指定します。

- *MM*/*DD*：*MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。
- *month week date*
  - **month**−月を指定します。January、February、March、April、May、June、July、August、September、October、November、December が指定できます。

- **week**−月で開始する週を指定します。first、second、third、fourth、fifth、last が指定できます。
- **day**−日を指定します。Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday が指定できます。

add-time: 標準時刻に追加する時間です。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

説明

clock summer-time コマンドは指定した期間サマータイムを使用します。

undo clock summer-time コマンドは設定を削除します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

装置を、ローカルシステム時間または NTP 時間ソースを使用するように設定可能です。

装置がローカルシステム時間を使用する場合、装置のシステム時間は以下の要素に依存します。

- ローカルタイムゾーン
- UTC 時間

システム時間を確認するには、**display clock** コマンドを使用します。

例

08/01 の 06:00:00 から 09/01 の 06:00:00 の間、システムの時間を 1 時間進めます。

<AP> system-view

[AP] clock summer-time PDT 6 08/01 6 09/01 1

関連コマンド

- **clock datetime**
- **clock timezone**
- **display clock**

1.1.4 clock timezone

Syntax

clock timezone *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

デフォルト

UTC 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

zone-name: タイムゾーン名を名前で指定します。大文字小文字を区別する 1～32 文字の文字列です。

add: UTC 時間（協定世界時：universal time coordinated）に対する正（+）のオフセットです。

minus: UTC 時間に対する負（-）のオフセットです。

zone-offset: UTC 時間に対するオフセットです。形式は *hh:mm:ss* （時/分/秒）です。*hh* の設定範囲は 0～23 です。mm の設定範囲は 0～59 です。ss の設定範囲は 0～59 です。*hh, mm, ss* において最初の 0 は省略可能です。*ss* が 00 の場合 *hh:mm* で表し、*mm* と *ss* が 00 の場合 *hh* で示します。たとえば 08:00:00 を指定する場合、*hh* に 8 を設定できます。

説明

clock timezone コマンドはローカルタイムゾーンを設定します。

undo clock timezone コマンドはデフォルトに戻します。

正しいシステムクロックの設定はネットワーク管理と通信に不可欠です。ネットワークで装置を動作させる前に、装置のシステム時間を設定してください。

装置を、ローカルシステム時間または NTP 時間ソースを使用するように設定可能です。

装置がローカルシステム時間を使用する場合、装置のシステム時間は以下の要素に依存します。

- ローカルタイムゾーン
- UTC 時間

システム時間を確認するには、**display clock** コマンドを使用します。

例

UTC より 5 時間進めたローカルタイムゾーン名を Z5 に設定します。

<AP> system-view

[AP] clock timezone Z5 add 5

関連コマンド

- **clock datetime**
- **clock summer-time**
- **display clock**

1.1.5 command

Syntax

command *id command*

undo command *id*

デフォルト

コマンドはジョブに割り当てられていません。

View

Job view

定義済みユーザロール

network-admin

パラメータ

id: コマンドの ID を指定します。設定範囲は 0～4294967295 です。コマンドの ID は job を一意に識別します。job のコマンドは昇順で実行されます。

command: job に割り当てられたコマンドを指定します。

説明

command コマンドはジョブにコマンドを割り当てます。

undo command コマンドはコマンドを取り消します。

コマンド（コマンド A）を job に割り当てるため、コマンド A の view に移行するコマンドを job に割り当ててください。

スケジュールのすべてのコマンドがコマンド構文に合致していることを確認してください。コマンドをジョブに割り当てる際、システムは構文を検査しません。

telnet コマンド、ftp コマンド、ssh2 コマンド、**monitor process** コマンドはスケジュール自動実行することはできません。

スケジュール自動実行機能はユーザがインタラクティブにコマンドの操作を扱うことができません。もしコマンドが”YES”あるいは”NO”の答えを要求する場合、システムはいつも”Y”あるいは”YES”が入力されます。もし文字列の入力が必要な場合、システムは自動的にデフォルト文字列を入力するか、デフォルト文字列がない場合、空の文字列を入力します。

コマンドが既存のコマンドの ID を使用する場合、既存のコマンドは置き換えられます。

例

job 名が backupconfig の job に、コンフィグレーションファイル startup.cfg を TFTP サーバ 192.168.100.11 にバックアップを行うコマンドを割り当てます。

<AP> system-view

[AP] scheduler job backupconfig

[AP-job-backupconfig] command 2 tftp 192.168.100.11 put flash:/startup.cfg backup.cfg

job 名が shutdownGE の job に GigabitEthernet 1/0/1 をシャットダウンするコマンドを割り当てます。

<AP> system-view

[AP] scheduler job shutdownGE

[AP-job-shutdownGE] command 1 system-view

[AP-job-shutdownGE] command 2 interface gigabitethernet 1/0/1

[AP-job-shutdownGE] command 3 shutdown

関連コマンド

scheduler job

1.1.6 copyright-info enable

Syntax

copyright-info enable

undo copyright-info enable

デフォルト

無効

メモ：

ソフトウェアバージョン 7.5.98 と 7.5.105 では、**undo copyright-info enable** が表示されます。
ソフトウェアバージョン 7.5.114 では、コンフィグ上では非表示です。

View

System view

定義済みユーザロール

network-admin

説明

copyright-info enable コマンドは著作権情報の表示を有効にします。

undo copyright-info enable コマンドは著作権情報の表示を無効にします。

例

著作権情報の表示を有効にします。

<AP> system-view

[AP] copyright-info enable

1.1.7 diag boot-info display

Syntax

diag boot-info display

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

diag boot-info display コマンドは装置の再起動履歴を表示します。

装置の再起動履歴は、直近で最大 10 件まで表示されます。

例

装置の再起動履歴を表示します。

<AP> diag boot-info display

```
********************************************************************************
PowerOn BootTimes   : 4
Watchdog BootTimes  : 0
Software BootTimes  : 118
Hardware BootTimes  : 0
MotherBoard BootTimes: 0
Backup BootTimes    : 0
SlotOut BootTimes   : 0
Current Boot Type   : Software-boot
Current Running Time: 0(s)
Running Time        : 132(d)20(h)
*** Boot History(Startup Time and Reason) ***
2021-12-16 05:52:52 User soft reboot
2021-12-15 23:52:44 User soft reboot
2021-12-15 23:50:42 User soft reboot
2021-12-15 23:49:51 User soft reboot
2021-12-08 06:26:08 User soft reboot
2021-12-08 06:20:09 User soft reboot
2021-02-15 17:32:12 User soft reboot
2021-02-13 16:26:48 User soft reboot
2021-02-09 12:33:54 User soft reboot
2021-01-23 14:18:54 Power on
```

表 1-1 コマンド出力

フィールド	説明
PowerOn BootTimes	Power onが原因で再起動した合計回数です。
Watchdog BootTimes	Watchdog rebootが原因で再起動した合計回数です。
Software BootTimes	soft rebootが原因で再起動した合計回数です。
Hardware BootTimes	Hard rebootが原因で再起動した合計回数です。
MotherBoard BootTimes	Master slotの合計再起動回数です。
Backup BootTimes	Standby slotの合計再起動回数です。
SlotOut BootTimes	Stanby slotが外れた合計回数です。

フィールド	説明
Current Boot Type	現在のBootタイプを示します。 ● Poweron-boot：ACアダプタやPoE給電による再起動を示します。 ● Software-boot：CLIやSNMPによる再起動を示します。 ● Watchdog-boot：watchdog rebootによる再起動を示します。 ● Hardware-boot：リセットボタン押下による再起動を示します。 ● Memory exhaust reboot：メモリ不足による再起動を示します。 ● Kernel exception soft reboot：カーネルの異常による再起動を示します。 ● Kernel deadloop soft reboot：カーネルスレッドのデッドループによって発生する再起動を示します。 ● DP/NSS switch soft reboot：DPモード、またはNSSモードを変更した場合の再起動を示します。 ● Unknown：再起動理由は不明です。
Current Running Time	直近のBootの動作時間を示します。
Running Time	合計の動作時間を示します。
Boot History(Startup Time and Reason)	装置の再起動履歴を示します。再起動理由については、表1-2を参照してください。

表 1-2 Boot History の Reason フィールドの説明

フィールド	説明
Power on	ACアダプタやPoE給電による再起動です。ACアダプタやPoE給電のケーブルが抜けたことによる再起動か、停電が発生した可能性があります。
User soft reboot:	CLIやSNMPによる再起動を示します。
User soft reboot(target restration)	周囲の電波状況が劣悪な環境である、またはそのほかの理由により、無線モジュールリセットのために再起動した可能性があります。
Hard reboot	リセットボタン押下による再起動を示します。
DP/NSS switch soft reboot	DPモード、またはNSSモードを変更した場合の再起動を示します。
Memory exhaust reboot	メモリ不足による再起動を示します。
Watchdog reboot	watchdog rebootによる再起動を示します。
Kernel exception soft reboot	カーネルの異常による再起動を示します。
Kernel deadloop soft reboot	カーネルスレッドのデッドループによって発生する再起動を示します。

関連コマンド

- **display version**

1.1.8 display clock

Syntax

display clock

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

システムの現在時刻、日付、タイムゾーン、サマータイムを表示するには、**display clock** コマンドを使用します。

例

ローカルタイムゾーンが指定されていないとき、システム時間を表示します。

<AP> display clock

```
10:09:00 UTC Fri 03/16/2017
```

ローカルタイムゾーン Z5 が指定されているとき、システム時間を表示します。

<AP> display clock

```
15:10:00 Z5 Fri 03/16/2017
Time Zone : Z5 add 05:00:00
```

ローカルタイムゾーン Z5 が指定され、PDT サマータイムが指定されているとき、システム時間を表示します。

<AP> display clock

```
15:11:00 Z5 Fri 03/16/2017
Time Zone : Z5 add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

関連コマンド

- **clock datetime**
- **clock timezone**
- **clock summer-time**

1.1.9 display copyright

Syntax

display copyright

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display clock コマンドは著作権表示します。

例

著作権情報を表示します。

<AP> display copyright

1.1.10 display cpu-usage

Syntax

display cpu-usage [**summary**]

display cpu-usage [**control-plane** | **data-plane**] [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

control-plane: コントロールプレーンの CPU 使用率の統計情報を表示します。このキーワードまたは data-plane キーワードを指定しない場合は、CPU 使用率の合計が表示されます。

data-plane: データプレーンの CPU 使用率の統計情報を表示します。このキーワードまたは control-plane キーワードを指定しない場合は、CPU 使用率の合計が表示されます。

summary: CPU 使用率の統計情報を表形式で表示します。このキーワードを指定しない場合、コマンドは CPU 使用率の統計情報をテキスト形式で表示されます。

説明

display cpu-usage コマンドは CPU 使用率の統計情報を表示します。

最新の 5 秒、1 分、5 分間隔の CPU 使用率に 2 つのハイフン (--) が表示されている場合、コマンドはデバイス上のデータベースからデータを取得できない可能性があります。後ほどコマンドを試してください。

起動後、装置は平均 CPU 使用率を以下の間隔で記録します。

- 5 秒
- 1 分
- 5 分

本コマンドは、最新の 5 秒間、1 分間、5 分間の CPU 使用率の平均値を表示します。

例

現在の CPU 使用率の統計情報をテキスト形式で表示します。

<AP> display cpu-usage

```
Unit CPU usage:
      1% in last 5 seconds
      1% in last 1 minute
      1% in last 5 minutes
```

表 1-3 コマンド出力

フィールド	説明
Unit CPU usage	CPU使用率統計情報
CPU	CPU番号
x% in last 5 seconds Last 5 sec	最後の5秒のCPU使用率の平均です。
y% in last 1 minute Last 1 min	最後の1分のCPU使用率の平均です。
z% in last 5 minutes Last 5 min	最後の5分のCPU使用率の平均です。

1.1.11 display cpu-usage history

Syntax

display cpu-usage history [**job** *job-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

job *job-id*: job の ID のプロセスを指定します。指定しない場合、すべてのプロセスのシステム全体の CPU 使用率履歴の統計情報を表示します。

説明

display cpu-usage history コマンドは CPU 使用率履歴の統計情報を表示します。

CPU 使用率のモニタリングが有効にされたのち、システムはある時間での CPU 使用率統計情報を取得し、履歴記録領域に統計結果を保存します。このコマンドは最後の 60 分間の CPU 使用率の統計情報レコードを座標で表示します。

Y 座標は、CPU 使用率を示します。もし統計情報が使用率のステップの倍数でない場合、もっとも近いステップに切り下げあるいは切り上げされます。たとえば CPU 使用率のステップが 5%である場合、統計情報が 53%である場合 55%に切り上げされます。統計情報が 52%である場合、50%に切り下げられます。

X 座標は時間を示します。

シャープ（#）は、ある時点における CPU 使用率を示します。ある時点上で#マークが 1 つ以上あるとき、一番高い位置の#マークが、現時点での CPU 使用率です。

例

CPU 使用率履歴の統計情報を表示します。

<AP> display cpu-usage history

```
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|           #
 10%|          ###  #
  5%|         ########
    ------------------------------------------------------------
            10       20       30       40       50       60  (minutes)
                   cpu-usage last 60 minutes (SYSTEM)
```

出力は以下のアイテムを示します。

- プロセス名：**SYSTEM**（全システムを示します。）
- 最新の 60 分間の CPU 使用率
  - 12 分前：5%
  - 13 分前：10%
  - 14 分前：15%
  - 15 分前：10%
  - 16 分前：5%
  - 17 分前：5%
  - 18 分前：10%
  - 19 分前：5%
  - その他の時間：2%または 2%未満

プロセス 1 の CPU 使用率履歴の統計情報を表示します。

<AP> display cpu-usage history job 1

```
100%|
 95%|
 90%|
 85%|
 80%|
 75%|
 70%|
 65%|
 60%|
 55%|
 50%|
 45%|
 40%|
 35%|
 30%|
 25%|
 20%|
 15%|
 10%|
  5%|                #
    ------------------------------------------------------------
            10       20       30       40       50       60  (minutes)
                   cpu-usage last 60 minutes (scmd)
```

出力は以下のアイテムを示します。

- プロセス名：**scmd**（[ ]内のプロセス名はカーネルプロセスを示します）
- 最新の 60 分間の CPU 使用率
  - 20 分前：5%
  - その他の時間：2%または 2%未満

関連コマンド

- **monitor cpu-usage enable**
- **monitor cpu-usage interval**

1.1.12 display device

Syntax

display device [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: 詳細ハードウェア情報を表示します。本キーワードを指定しない場合、概要情報を表示します。

説明

display device コマンドは装置情報を表示します。

例

装置情報を表示します。

<AP> display device

```
Slot No.  Subslot No. Board Type       Status    Max Ports
1          0           QX-W610          Normal    3
```

表 1-4 コマンド出力

フィールド	説明
Board Type	デバイスのハードウェアタイプ
Status	デバイスステータス: • **Illegal:**The device is not operating correctly • **Normal:**The device is operating correctly.
Max Ports	ハードウェアタイプ

1.1.13 display device manuinfo

Syntax

display device manuinfo

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display device manuinfo コマンドは装置の電子ラベル情報を表示します。

電子ラベル情報とは、装置またはカードのプロファイルです。シリアル番号、製造年月日、MAC アドレス、ベンダ名といった固定的な設定情報を含んでいます。データはデバッグまたはテスト中に記憶媒体に書き込まれます。

例

装置の電子ラベル情報を表示します。

<AP> display device manuinfo

```
DEVICE_NAME:QX-W610
DEVICE_SERIAL_NUMBER:210235A1ABC166000028
MAC_ADDRESS:8455-3110-9FD8
MANUFACTURING_DATE:2023-06-04
VENDOR_NAME:NEC
```

表 1-5 コマンド出力

フィールド	説明
DEVICE_NAME	装置名
DEVICE_SERIAL_NUMBER	シリアル番号
MAC_ADDRESS	MACアドレス
MANUFACTURING_DATE	製造年月日
VENDOR_NAME	ベンダ名

1.1.14 display diagnostic-information

Syntax

display diagnostic-information [**hardware** | **infrastructure** | **l2** | **l3** | **service**] [**key-info**] [*filename*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

hardware: ハードウェアに関する稼働状態の診断情報を表示します。

infrastructure: 基本機能に関する稼働状態の診断情報を表示します。

l2: レイヤ 2 機能に関する稼働状態の診断情報を表示します。

l3: レイヤ 3 機能に関する稼働状態の診断情報を表示します。

service: 上位レイヤ機能に関する稼働状態の診断情報を表示します。

key-info: 重要な動作情報だけを表示または保存します。例外が発生した場合や、デバイスが長時間動作した後は、デバイスの動作情報が大量になることがあります。このキーワードを指定すると、コマンドの実行時間が短縮され、重要な動作情報に集中できるようになります。このキーワードを指定しない場合、コマンドは重要な動作情報と重要でない動作情報の両方を表示または保存します。

filename: 情報をファイルに保存します。*filename* 引数には、拡張子.tar.gz を使用する必要があります。この引数を指定しない場合、情報をファイルに保存するか、情報を表示するかを選択するように求められます。

説明

display diagnostic-information コマンドはデバイス診断情報を表示または保存します。

診断とトラブルシューティングにあたり、稼働統計情報を収集するために以下の方法のうち 1 つを使用します。

- 機能ごと、またはモジュールごとの稼働情報を収集するため、個別の display コマンドを使用します。
- 複数またはすべての機能とハードウェアのモジュールの稼働情報を収集するため、**display diagnostic-information** コマンドを使用します。

ストレージスペースを節約するために、情報をファイルに保存する前に、このコマンドは自動的に情報を圧縮します。ファイル内容を見るには

1) tar extract コマンドでファイルを解凍します。

2) gunzip コマンドでファイルを解凍します。

3)　解凍したファイルの内容を more コマンドで表示します。

関連コマンド

- **gunzip**
- **more**
- **tar extract**

1.1.15 display memory

Syntax

display memory [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display memory コマンドは装置のメモリ使用率を表示します。

summary: メモリ使用量に関する簡単な情報を表示します。このキーワードを指定しない場合、コマンドはメモリ使用量に関する詳細情報を表示します

コマンド出力の 1 行ですべてのフィールドに 2 つのハイフン (--) が表示された場合、デバイス上のデータベースからデータを取得できないことがあります。後ほどコマンドを実行してください。

例

メモリ使用率を表示します。

<AP> display memory

簡単なメモリ使用状況情報を表示します。

<AP> display memory summary

```
display memory summary Memory statistics are measured in KB:
CPU       Total       Used        Free    Buffers  Caches FreeRatio
0         1029476 325012      704464      2404    143008       68.4%
```

表 1-6 コマンド出力

フィールド	説明
Mem	メモリ使用率

フィールド	説明
Total	割り当てることができる物理メモリサイズの合計 メモリサイズは2つの部分に分けられる。 1番目は単独でカーネルコード、カーネル管理に使用される。2番目は稼働サービスモジュールのようなタスク、ファイルの格納に使用される。2番目のサイズはトータルの物理メモリサイズから1番目のメモリサイズを引いたサイズとなる。
Used	使用されている物理メモリ
Free	使用されていない物理メモリ
Shared	プロセスによって共有されている物理メモリ
Buffers	バッファで使用されている物理メモリ
Cached	キャッシュで使用されている物理メモリ
FreeRatio	使用されていないメモリの割合です。
-/+ Buffers/Cache	-/+ Buffers/Cache:Used = Mem:Used – Mem:Buffers – Mem:Cached ここで物理メモリはアプリケーションで使用されていることを示す -/+ Buffers/Cache:Free = Mem:Free + Mem:Buffers + Mem:Cached ここで物理メモリはアプリケーションで使用可能であることを示す
Swap	スワップメモリ

1.1.16 display memory-threshold

Syntax

display memory-threshold

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display memory-threshold コマンドは装置のメモリしきい値とメモリ使用率通知の統計情報を表示します。

メモリ使用率通知の詳細は以下のログ情報を参照してください。

MEM_EXCEED_THRESHOLD あるいは MEM_BELOW_THRESHOLD

例

装置のメモリしきい値とメモリ使用率通知の統計情報を表示します。

<AP> display memory-threshold

```
Memory usage threshold: 100%
Free memory threshold:
   Minor: 16M
   Severe: 8M
   Critical: 4M
   Normal: 32M
Current memory state: Normal
Event statistics:
 [Back to normal state]
   First notification: 0.0
   Latest notification: 0.0
   Total number of notifications sent: 0
 [Enter minor low-memory state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Back to minor low-memory state]
   First notification at: 0.0
   Latest notification at: 0.0
   Total number of notifications sent: 0
 [Enter severe low-memory state]
```

```
  First notification at: 0.0
  Latest notification at: 0.0
  Total number of notifications sent: 0
[Back to severe low-memory state]
  First notification at: 0.0
  Latest notification at: 0.0
  Total number of notifications sent: 0
[Enter critical low-memory state]
  First notification at: 0.0
  Latest notification at: 0.0
  Total number of notifications sent: 0
```

1.1.17 display scheduler job

Syntax

display scheduler job [*job-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

job-name: job の名前を指定します。設定範囲は 1～47 文字で、大文字小文字を区別します。指定しない場合、すべての job の設定情報を表示します。

説明

display scheduler job コマンドは job 設定情報を表示します。

例

すべての job の設定情報を表示します。

<AP> display scheduler job

```
Job name: saveconfig
 copy startup.cfg backup.cfg

Job name: backupconfig

Job name: creat-VLAN100
 system-view
```

```
 vlan 100
```

// 出力では、装置は 3 つの job があることを示します。最初の job には 1 つのコマンドがあります。2 番目の job にはコマンドがありません。3 番目の job には 2 つのコマンドがあります。job は空白行で区切られます。

1.1.18 display scheduler logfile

Syntax

display scheduler logfile

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display scheduler logfile コマンドは job 実行のログ情報を表示します。

例

実行された job のログ情報を表示します。

<AP> display scheduler logfile

```
Logfile Size: 1902 Bytes.

Job name       : shutdown
Schedule name   : shutdown
Execution time  : Tue Feb 27 10:44:42 2017
Completion time : Tue Feb 27 10:44:47 2017
------------------------------ Job output ----------------------------------
-
```

<AP> system-view

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

[AP] interface rang gigabitethernet 1/0/1

[AP-if-range] shutdown

表 1-7 コマンド出力

フィールド	説明
Logfile Size	ログファイルのサイズ。byteで表示される。
Schedule name	jobが所属するスケジュール
Execution time	jobが開始されたときの時間

フィールド	説明
Completion time	jobが完了したときの時間 jobが実行されなかった、あるいはjobにコマンドがない場合、このフィールドは表示されない
Job output	jobのコマンドと出力

1.1.19 display scheduler reboot

Syntax

display scheduler reboot

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display scheduler reboot コマンドは自動再起動のスケジュールを表示します。

例

装置の自動再起動スケジュールを表示します。

<AP> display scheduler reboot

```
System will reboot at 16:32:00 05/23/2017 (in 1 hours and 39 minutes).
```

関連コマンド

- **scheduler reboot at**
- **scheduler reboot delay**

1.1.20 display version

Syntax

display version

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display version コマンドはシステムバージョン情報を表示します。

例

システムのバージョン情報を表示します。

<AP> display version

Comware Software, Version 7.5.114

QX-W610 uptime is 0 weeks, 0 days, 23 hours, 37 minutes

Last reboot reason : User soft reboot

Boot image: flash:/qx-w610-boot-v75114.bin

Boot image version: 7.5.114

  Compiled Nov 11 2024 16:00:00

System image: flash:/qx-w610-system-v75114.bin

System image version: 7.5.114

  Compiled Nov 11 2024 16:00:00

with 1 ARM 1.0GHz Processor

1024M bytes DDR3

256M bytes NandFlash Memory

Current running mode: FAT AP

Next startup mode: FAT AP

Hardware Version is Ver.A

Basic Bootrom Version is 1.03

Extend Bootrom Version is 1.03

[Subslot 0]QX-W610 Hardware Version is Ver.A

[SLOT 1]GE1/0/1 (Hardware)Ver.A, (Driver)1.0

[SLOT 1]RADIO1/0/1 (Hardware)Ver.A, (Driver)1.0

[SLOT 1]RADIO1/0/2 (Hardware)Ver.A, (Driver)1.0

表 1-8 フィールドの説明

フィールド	説明
Comware Software, Version 7.x.yyy	装置のバージョンを示します。例えば、「Comware Software, Version 7.5.114」だった場合は、装置のバージョンがv7.5.114であることを示します。
QX-W610 uptime is 1 weeks, 2 days, 10 hours, 10 minutes	装置がどのくらいの時間稼働しているかを示します。 例えば、「QX-W610 uptime is 1 weeks, 2 days, 10 hours, 10 minutes」だった場合は、1週間と2日、10時間10分稼働していることを示します。
Last reboot reason	デバイスが最後に再起動した理由を示します。理由についての説明は表 1-9を参照してください。

表 1-9 Last reboot reason のフィールドの説明

フィールド	説明
Power on	ACアダプタやPoE給電による再起動です。ACアダプタやPoE給電のケーブルが抜けたことによる再起動か、停電が発生した可能性があります。
User soft reboot	CLI (**reboot** コマンド) やSNMPによる再起動を示します。 または、周囲の電波状況が劣悪な環境である、またはそのほかの理由により、無線モジュールリセットのために再起動した可能性があります。意図しない再起動の場合は、**diag boot-info display** コマンドを実行して、Boot History フィールドを確認してください。
Hard reboot	リセットボタン押下による再起動を示します。
DP/NSS switch soft reboot	DPモード、またはNSSモードを変更した場合の再起動を示します。
Memory exhaust reboot	メモリ不足による再起動を示します。
Watchdog reboot	watchdog rebootによる再起動を示します。
Kernel exception soft reboot	カーネルの異常による再起動を示します。
Kernel deadloop soft reboot	カーネルスレッドのデッドループによって発生する再起動を示します。

注意：

QX-W610 では、v7.5.98 と v7.5.105 では、周囲の電波状況が劣悪な環境である、またはそのほかの理由により、無線モジュールリセットのための再起動が発生した場合、display version コマンドの Last reboot reason フィールドでは、「User soft reboot」と表示されます。意図しない再起動が発生した場合は、diag boot-info display を実行して、Boot History フィールドを確認してください。

関連コマンド

- **diag boot-info display**

1.1.21 header

Syntax

header { **legal** | **login** | **motd** | **shell** } *text*

undo header { **legal** | **login** | **motd** | **shell** }

View

System view

定義済みユーザロール

network-admin

パラメータ

legal: ユーザがユーザ名およびパスワードを CLI にアクセスして入力する前にバナーを設定します。

login: ログインユーザによってパスワードまたは scheme 認証される前にバナーを設定します。

motd: **legal** バナーが表示される前に greeting（あいさつ）バナーを設定します。

shell: 非モデムログインユーザが user view に移行する際に表示されるバナーを設定します。

text: バナーメッセージです。パラメータあるいは複数行の 2 つの形式で入力できます。詳細は、オペレーションマニュアルのセクション 2 *システム管理"“装置管理”*を参照してください。

説明

header コマンドはバナーを設定します。

undo header コマンドはバナーを削除します。

例

legal バナー、login バナー、MOTD バナー、shell バナーを作成します。

<AP> system-view

[AP] header legal

```
Please input banner content, and quit with the character '%'.
Welcome to legal (header legal)%
```

[AP] header login

```
Please input banner content, and quit with the character '%'.
Welcome to login(header login)%
```

[AP] header motd

```
Please input banner content, and quit with the character '%'.
Welcome to motd(header motd)%
```

[AP] header shell

```
Please input banner content, and quit with the character '%'.
Welcome to shell(header shell)%
```

本例では、パーセント記号（%）は各バナーの開始及び終了文字で、バナー内には含まれません。

設定をテストするために telnet を実行します。ログインバナーは、password または scheme ログイン認証が設定されている場合のみ表示されます。

```
Welcome to legal (header legal)
 Press Y or ENTER to continue, N to exit.

Welcome to motd(header motd)

Welcome to login(header login)

Login authentication


Password:

Welcome to shell(header shell)
```

1.1.22 job

Syntax

job *job-name*

undo job *job-name*

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

job-name: job 名を指定します。設定範囲は 1～47 文字で、大文字、小文字を区別します。

説明

job コマンドはスケジュール自動実行機能のスケジュールに job を割り当てます。

undo job コマンドは job を削除します。

スケジュールに複数の job を割り当てることができます。スケジュールの job は連続して実行されます。

スケジュールに割り当てられる job はあらかじめ作成されている必要があります。job を作成する場合、**scheduler job** コマンドを使用します。

例

スケジュール saveconfig に job 名が save-job の job を割り当てます。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] job save-job

関連コマンド

- **scheduler job**
- **scheduler schedule**

1.1.23 memory-threshold

Syntax

memory-threshold [**ratio**] **minor** *minor-value* **severe** *severe-value* **critical 4 normal** *normal-value*

undo memory-threshold

デフォルト

Minor alarm threshold　: 16 MB.

Severe alarm threshold　: 8 MB.

Critical alarm threshold　: 4 MB.

Normal state threshold　: 32 MB.

View

System view

定義済みユーザロール

network-admin

パラメータ

ratio： 空きメモリのしきい値をパーセントで指定します。このキーワードを指定しない場合、コマンドは空きメモリのしきい値を MB 単位で設定します。

minor *minor-value*: **minor** アラームのしきい値を指定します。設定範囲は 0～489 です。しきい値は **normal** しきい値以下にする必要があります。0 に指定すると **minor** アラーム機能を無効にします。

severe *severe-value*: **severe** アラームのしきい値を指定します。設定範囲は **minor** アラームのしきい値によって変わります。しきい値は **minor** しきい値以下にする必要があります。0 に指定すると **severe** アラーム機能を無効にします。

critical 4: **critical** アラームのしきい値を指定します。設定は 4 を指定してください。
normal *normal-value*: **normal** アラームのしきい値を指定します。設定範囲は **minor** アラームのしきい値によって変わります。しきい値はメモリサイズの合計以下にする必要があります。

注意：

QX-W610 では、memory-threshold コマンドの critical パラメータを選択することができますが、設定変更した場合に装置が再起動する可能性があります。critical パラメータはデフォルト値 (4MB) で運用してください。

説明

memory-threshold コマンドは空きメモリ容量のしきい値を設定します。

undo memory-threshold コマンドはデフォルトに戻します。

正常な動作とメモリ使用率を改善するため、システムはリアルタイムで使用可能なメモリサイズをモニタします。しきい値が超過すると、モジュールあるいはプロセスで対策を行うことができるように、システムはアラーム通知あるいはアラーム解除通知を関係するモジュールあるいはプロセスに通知します。しきい値の詳細はオペレーションマニュアルのセクション 2 *システム管理“装置管理”*を参照してください。

例

minor アラームを 64MB、severe アラームを 48MB、critical アラームを 4 MB、normal アラームを 96MB に設定します。

<AP> system-view

[AP] memory-threshold minor 64 severe 48 critical 4 normal 96

注意：

QX-W610 では、memory-threshold コマンドの critical パラメータを選択することができますが、設定変更した場合に装置が再起動する可能性があります。critical パラメータはデフォルト値 (4MB) で運用してください。

関連コマンド

display memory-threshold

1.1.24 monitor cpu-usage enable

Syntax

monitor cpu-usage enable

undo monitor cpu-usage enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

monitor cpu-usage enable コマンドは CPU 使用率の監視を有効にします。

undo monitor cpu-usage enable コマンドは CPU 使用率の監視を無効にします。

CPU 使用率の監視を有効にしたのち、**monitor cpu-usage interval** コマンドで指定したサンプリング間隔で CPU 使用率を監視、保存します。最新の CPU 使用率を表示する場合、**display cpu-usage history** コマンドを使用します。

例

CPU 使用率の監視を有効にします。

<AP> system-view

[AP] monitor cpu-usage enable

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage interval**

1.1.25 monitor cpu-usage interval

Syntax

monitor cpu-usage interval *interval*

デフォルト

1 分

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: CPU 使用率のサンプリング間隔を指定します。5Sec、1Min、5Min から指定します。5Sec は 5 秒、1Min は 1 分、5Min は 5 分です。

説明

monitor cpu-usage interval コマンドは CPU 使用率のサンプリング間隔を設定します。

CPU 使用率の監視を有効にしたのち、指定したサンプリング間隔で CPU 使用率を監視し、保存します。最新の CPU 使用率を表示する場合、**display cpu-usage history** コマンドを使用します。

例

CPU 使用率のサンプリング間隔を 5 秒に設定します。

<AP> system-view

[AP] monitor cpu-usage interval 5Sec

関連コマンド

- **display cpu-usage configuration**
- **display cpu-usage history**
- **monitor cpu-usage enable**

1.1.26 monitor cpu-usage threshold

Syntax

monitor cpu-usage threshold *severe-threshold*

undo monitor cpu-usage threshold

デフォルト

99%

View

System view

定義済みユーザロール

network-admin

パラメータ

severe-threshold: 重大な CPU 使用率のしきい値をパーセンテージで指定します。この引数の値の範囲は 2 から 100 です。

説明

monitor cpu-usage threshold コマンドは CPU 使用率のしきい値を設定します。

undo monitor cpu-usage threshold コマンドはデフォルトに戻します。

⚠ **注意：**

CPU 使用率のしきい値を低すぎる値に設定すると、デバイスは容易にしきい値に到達します。通常のサービス処理が影響を受けます。

装置は 1 分間隔で CPU 使用率をサンプリングします。サンプリングした値と CPU の使用率のしきい値を比較します。CPU 使用率のしきい値より大きい場合、装置は trap を送信します。

例

CPU 使用率アラームしきい値を 90%に設定します。

<AP> system-view

[AP] monitor cpu-usage threshold 90

関連コマンド

display cpu-usage configuration

1.1.27 password-recovery enable

Syntax

password-recovery enable

undo password-recovery enable

デフォルト

有効

メモ：

ソフトウェアバージョン 7.5.98、7.5.105 では、コンフィグ上では **password-recovery enable** が表示されます。
ソフトウェアバージョン 7.5.114 を含む以降のソフトウェアではコンフィグ上では非表示です。

View

System view

定義済みユーザロール

network-admin

説明

password-recovery enable コマンドはパスワードリカバリ機能を有効にします。

undo password-recovery enable コマンドはパスワードリカバリ機能を無効にします。

パスワードリカバリ機能は Boot ROM メニューからデバイス構成と SDRAM へのアクセスを制御できます。

パスワードリカバリ機能が有効である場合、コンソールからのユーザは認証なしで装置にアクセスでき、新しいパスワードを設定することができます。

パスワードリカバリ機能が無効である場合、コンソールからのユーザは、新しいパスワードを設定する前に、工場出荷状態にする必要があります。工場出荷状態に戻すと次回に起動で使用するコンフィグレーションファイルを削除します。

本機能は、主に管理者が設定したパスワードを忘れたときに使用します。パスワードリカバリ機能が有効な場合、保存してある current-configuration や super password を読み込まずに装置を起動できます。コンフィグを読み込まずに起動する操作は Boot メニューから行います

例

パスワードリカバリ機能を無効にします。

<AP> system-view

[AP] undo password-recovery enable

1.1.28 reboot

Syntax

reboot [**force**]

View

User view

定義済みユーザロール

network-admin

パラメータ

force: ソフトウェアの確認を行わず、すぐに装置を再起動します。本キーワードを指定しない場合、システムは、再起動によってデータ紛失あるいはシステムの故障が発生するかどうかを確認します。たとえば、システムはメインシステムソフトウェアのファイルが存在するか、および書き込み操作が記憶媒体で進行中であるかどうか確認します。再起動によって問題は発生すると認識した場合、システムは装置の再起動を行いません。

説明

reboot コマンドは装置を再起動します。

⚠ **注意**:

- 再起動によってネットワークサービスが中断されることがあります。
- デバイスに障害が発生した場合、または **force** キーワードを指定しないで再起動コマンドを実行しても再起動を正しく実行できない場合にのみ、**force** キーワードを使用します。**force** キーワードを指定した再起動コマンドは、データ保護を実行しないため、ファイルシステムが破損する可能性があります。

メインスタートアップソフトウェアイメージが破損または欠落している場合は、**reboot** コマンドを実行する前に、メインスタートアップソフトウェアイメージのセットを再指定する必要があります。

例

装置を再起動します。プロンプトで実行中のコンフィギュレーションを保存します。

<<AP> reboot

```
Start to check configuration with next startup configuration file, please
wait.........DONE!
```

Current configuration will be lost after the reboot, save current configuration? [Y/N]:y

Please input the file name(*.cfg)[flash:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):

flash:/startup.cfg exists, overwrite? [Y/N]:y

```
Validating file. Please wait...
Configuration is saved to flash successfully.
```

This command will reboot the device. Continue? [Y/N]:y

```
Now rebooting, please wait...
```

ソフトウェアチェックを行わず、すぐに装置を再起動します。

<AP> reboot force

A forced reboot might cause the storage medium to be corrupted. Continue? [Y/N]:y

```
Now rebooting, please wait..
```

関連コマンド

display system stable state

1.1.29 reset scheduler logfile

Syntax

reset scheduler logfile

View

User view

定義済みユーザロール

network-admin

説明

reset scheduler logfile コマンドはスケジュール自動実行機能のログ情報の削除を行います。

例

スケジュール自動実行機能のログ情報を削除します。

<AP> reset scheduler logfile

関連コマンド

display scheduler logfile

1.1.30 restore factory-default

Syntax

restore factory-default

View

User view

定義済みユーザロール

network-admin

説明

restore factory-default コマンドは装置を工場出荷時のデフォルト状態に復元します。

注意：

このコマンドは注意して使用してください。デバイスを別の用途で使用する場合、または他の方法を使用してデバイスのトラブルシューティングを行うことができない場合のみ、このコマンドを使用してください。

例

装置を工場出荷時のデフォルト状態に復元します。

<AP> restore factory-default

```
This command will restore the system to the factory default configuration and
clear the operation data, and forcibly reboot the system. Continue [Y/N]:y
Restoring the factory default configuration. This process might take a few
minutes. Please wait....Done.
The system is rebooting...
```

1.1.31 scheduler job

Syntax

scheduler job *job-name*

undo scheduler job *job-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

job-name: job 名を指定します。設定範囲は 1～47 文字で大文字、小文字を区別します。

説明

scheduler job コマンドはスケジュール自動実行機能の job を作成し、job view に移行します。すでに job が存在する場合、直接 job view に移行します。

undo scheduler job コマンドは job を削除します。

job は複数のスケジュールから参照可能です。job view で job にコマンドを割り当てることができます。

例

job 名が backupconfig の job を作成し、job view に移行します。

<AP> system-view

[AP] scheduler job backupconfig

[AP-job-backupconfig]

関連コマンド

- **command**
- **scheduler schedule**

1.1.32 scheduler logfile size

Syntax

scheduler logfile size *value*

デフォルト

16KB

View

System view

定義済みユーザロール

network-admin

パラメータ

value: job を実行するログファイルのサイズを KB で設定します。設定範囲は 16～1024 です。

説明

scheduler logfile size コマンドはスケジュール自動実行機能の job を実行するログファイルのサイズを設定します。

job を実行するログファイルは、job が実行される情報を保存します。ファイルの容量が一杯である場合、古い記録が削除され、新しい記録が保存されます。もしファイルサイズよりもログファイルのサイズが大きい場合、実行される情報はファイルに保存されません。

例

job を実行するログファイルのサイズを 32KB に設定します。

<AP> system-view

[AP] scheduler logfile size 32

関連コマンド

display scheduler logfile

1.1.33 scheduler reboot at

Syntax

scheduler reboot at *time* [*date*]

undo scheduler reboot

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 再起動する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

date: 再起動する日時を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。*YYYY* の設定範囲は 2000～2035 です。*MM* の設定範囲は 1～12 です。*DD* の設定範囲は月によって変わります。

説明

scheduler reboot at コマンドはスケジュール再起動機能の日時、時間を指定します。

undo scheduler reboot コマンドはスケジュール再起動機能の設定を削除します。

注意：

装置を再起動するとネットワークサービスが中断されます。

date 引数が指定されていないときは、以下の動作を行います。

- 再起動時間が現在時刻より遅い場合、再起動は当日の再起動時間に行われます。
- 再起動時間が現在時刻より早い場合、再起動は次の日の再起動時間に行われます。

データ保護のため、ファイルの操作を実行している間、システムは装置の再起動を行いません。

装置はスケジュール再起動機能を 1 回のみサポートします。もし **schedule reboot delay** コマンドと **scheduler reboot at** コマンドの両方が設定されている場合、あるいはどちらかのコマンドを複数回設定した場合、最後に設定したコマンドが適用されます。

例

装置を PM12:00 に再起動します。現在時刻は 2011 年 6 月 6 日 11:43 であると仮定します。

<AP> scheduler reboot at 12:00

```
Reboot system at 12:00:00 06/06/2011 (in 0 hours and 16 minutes). Confirm?
[Y/N]:
```

関連コマンド

scheduler reboot delay

1.1.34 scheduler reboot delay

Syntax

scheduler reboot delay *time*

undo scheduler reboot

デフォルト

設定なし

View

User view

定義済みユーザロール

network-admin

パラメータ

time: 再起動する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。パラメータは 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。

説明

scheduler reboot delay コマンドはスケジュール再起動機能の再起動遅延時間を指定します。

undo scheduler reboot コマンドはスケジュール再起動機能の再起動遅延時間を削除します。

⚠ **注意**：

装置を再起動するとネットワークサービスが中断されます。

データ保護のため、ファイルの操作を実行している間、システムは装置の再起動を行いません。

装置はスケジュール再起動機能を 1 回のみサポートします。もし **schedule reboot delay** コマンドと **scheduler reboot at** コマンドの両方が設定されている場合、あるいはどちらかのコマンドを複数回設定した場合、最後に設定したコマンドが適用されます。

例

装置を 88 分後に再起動します。現在時刻は 2017 年 6 月 6 日の 11:48 であると仮定します。

<AP> scheduler reboot delay 88

```
Reboot system at 13:16 06/06/2017(in 1 hours and 28 minutes). Confirm? [Y/N]:
```

1.1.35 scheduler schedule

Syntax

scheduler schedule *schedule-name*

undo scheduler schedule *schedule-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

schedule-name: スケジュール名を指定します。設定範囲は 1～47 文字で大文字、小文字を区別します。

説明

scheduler schedule コマンドはスケジュール自動実行機能のスケジュールを作成し、schedule view に移行します。すでにスケジュールが存在する場合はすぐに schedule view に移行します。

undo scheduler schedule コマンドはスケジュールを削除します。

管理に影響を与えずに自動的にコマンドあるいはコマンドセットを装置が実行するように、スケジュールを設定することができます。

スケジュールを設定するには以下を行います。

1) **scheduler job** コマンドを使用して job を作成します。
2) job view で **command** コマンドを使用して job にコマンドを割り当てます。
3) **scheduler schedule** コマンドを使用してスケジュールを作成します。
4) schedule view で **job** コマンドを使用してスケジュールに job を割り当てます。複数の job をスケジュールに割り当てることができます。job はすでに作成している必要があります。
5) schedule view で **user-role** コマンドを使用してスケジュールにユーザロールを割り当てます。スケジュールに最大 64 のユーザロールを割り当てることができます。
6) schedule view で **time at** コマンド、**time once** コマンド、あるいは **time repeating** コマンドを使用して、スケジュールを実行する時間を指定します。1 つのスケジュールに 1 つの実行時間のみ指定することができます。

例

スケジュール名が saveconfig のスケジュールを作成します。

<AP> system-view

[AP] scheduler schedule saveconfig

関連コマンド

- **job**
- **time at**
- **time once**

1.1.36 shutdown-interval

Syntax

shutdown-interval *interval*

undo shutdown-interval

デフォルト

30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: 検出間隔を指定します。設定範囲は 0～300 秒です。0 秒に設定すると検出を行いません。

説明

shutdown-interval コマンドはポートの状態検出タイマを設定します。

undo shutdown-interval コマンドはデフォルトに戻します。

プロトコルによってポートがシャットダウンされる際、装置はポート状態検出タイマを開始します。タイマ経過後、装置はポートの物理状態を反映するため、ポートを起動します。

ポートの検出期間にタイマを変更した場合、装置は新しい設定 T1 とポートがシャットダウンしてから経過した時間 T を比較します。

もし T<T1 の場合、ポートは T1-T 秒後に起動します。

もし T>=T1 の場合、ポートはすぐに起動します。

たとえば、ポートがシャットダウンしてから 2 秒後にタイマを 30 秒から 10 秒に変更した場合、ポートは 8 秒後に起動します。ポートがシャットダウンしてから 10 秒後にタイマを 30 秒から 2 秒に変更した場合、ポートはすぐに起動します。

例

ポートの状態を検出する検出間隔を 100 秒に設定します。

<AP> system-view

[AP] shutdown-interval 100

1.1.37 sysid

Syntax

sysid *system-id*

undo sysid

デフォルト

sysid は設定されていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

system-id: 装置のシステム ID を指定します。この引数を使用して、デバイスの位置や機能、またはその他の情報を示すことができます。

説明

sysid コマンドは装置のシステム ID を設定します。

undo sysid コマンドはデフォルトに戻します。

例

装置のシステム ID を position-hall に設定します。

<AP> system-view

[AP] sysid positon-hall

1.1.38 sysname

Syntax

sysname *sysname*

undo sysname

デフォルト

装置名

View

System view

定義済みユーザロール

network-admin

パラメータ

sysname: 装置名を指定します。設定範囲は 1～64 文字です。

説明

sysname コマンドは装置名を設定します。

undo sysname コマンドはデフォルトに戻します。

装置名はネットワークの装置を識別し、CLI の user view のプロンプトとして使用されます。装置名が AP である場合、user view のプロンプトは<AP>です。

例

装置名を R2000 に設定します。

<AP> system-view

[AP] sysname R2000

[R2000]

1.1.39 time at

Syntax

time at *time date*

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

time: スケジュールを自動で実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

date: スケジュールを自動で実行する実行日を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。YYYY の設定範囲は 2000～2035 です。MM の設定範囲は 1～12 です。DD の設定範囲は月によって変わります。

説明

time at コマンドは 1 回のみのスケジュール自動実行機能の実行日と時間を指定します。

undo time コマンドはスケジュール自動実行機能の実行日と時間の設定を削除します。

指定時間（実行日と時間）は現在時刻よりも後にする必要があります。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

2017 年 5 月 11 日の AM01:01 にスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time at 1:1 2017/05/11

関連コマンド

scheduler schedule

1.1.40 time once

Syntax

time once at *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]

time once delay *time*

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。

month-date *month-day*: 月日を指定します。設定範囲は 1～31 です。当月に指定した日が存在しない場合、翌月の該当する日が適用されます。

week-day *week-day*&<1-7>: スケジュールを実行する曜日を指定します。半角スペースで区切り、曜日を最大 7 つまで指定します。値は Mon、Tue、Wed、Thu、Fri、Sat、Sun です。

delay *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。パラメータは 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。

説明

time once コマンドは 1 回のみのスケジュール自動実行機能の複数の実行日と時間を指定します。

undo time コマンドはスケジュール自動実行機能の実行日と時間の設定を削除します。
指定された時間が過ぎている場合、次の日の指定された時間が適用されます。

指定された月日が過ぎている場合、次の月の指定された日が適用されます。

指定された曜日が過ぎている場合、次の週の指定された曜日が適用されます。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

15:00 にスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time once at 15:00

```
Schedule starts at 15:00 5/11/2011.
```

今月の 15 日後の 15:00 にスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time once at 15:00 month-date 15

次の月曜日、金曜日の PM12:00 にスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time once at 12:00 week-day mon fri

10 分後にスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time once delay 10

関連コマンド

scheduler schedule

1.1.41 time repeating

Syntax

time repeating [**at** *time* [*date*]] **interval** *interval*

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>]

undo time

デフォルト

設定なし

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

at *time*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* です。*hh* の設定範囲は 0～23 です。*mm* の設定範囲は 0～59 です。指定しない場合、現在のシステム時間が指定されます。

date: スケジュールを定期的に自動で実行する開始日を指定します。形式は *MM*/*DD*/*YYYY* あるいは *YYYY*/*MM*/*DD* です。YYYY の設定範囲は 2000～2035 です。MM の設定範囲は 1～12 です。DD の設定範囲は月によって変わります。指定しない場合、指定した時間になったときの最初の日が指定されます。

interval *interval*: スケジュールを実行する時間を指定します。形式は *hh*:*mm* あるいは *mm* です。*mm* は 6 文字まで設定することができます。形式が *hh*:*mm* である場合、*mm* の設定範囲は 0～59 です。形式が *mm* である場合、パラメータは 1 分以上にする必要があります。

month-date [*month-day* | **last**]: 今月の日を指定します。設定範囲は 1～31 です。今月の日で指定した日が存在しない場合、次の月の該当する日が適用されます。

week-day *week-day*&<1-7>: スケジュールを実行する曜日を指定します。半角スペースで区切り、曜日を最大 7 つまで指定します。値は Mon、Tue、Wed、Thu、Fri、Sat、Sun です。

説明

time repeating コマンドは定期的にスケジュールを実行するタイムテーブルを指定します。

undo time コマンドはスケジュール自動実行機能の時間の設定を削除します。

time repeating [**at** *time* [*date*]] **interval** *interval* コマンドは 1 日内の指定した時間で定期的にスケジュールを実行するように設定します。

time repeating at *time* [**month-date** [*month-day* | **last**] | **week-day** *week-day*&<1-7>] コマンドは月あるいは曜日内の指定した日で定期的にスケジュールを実行するように設定します。

time at コマンド、**time once** コマンド、**time repeating** コマンドは、同時に設定することはできません。最後に設定したコマンドが適用されます。

例

本日の 8:00 から 1 時間ごとにスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time repeating at 8:00 interval 60

毎日 PM12:00 にスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time repeating at 12:00

毎月 5 日の AM8:00 にスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time repeating at 8:00 month-date 5

毎月最終日の AM8:00 にスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time repeating at 8:00 month-date last

各金曜日と各土曜日の AM8:00 にスケジュール saveconfig を実行するように設定します。

<AP> system-view

[AP] scheduler schedule saveconfig

[AP-schedule-saveconfig] time repeating at 8:00 week-day fri sat

関連コマンド

scheduler schedule

1.1.42 user-role

Syntax

user-role *role-name*

undo user-role [*role-name*]

デフォルト

スケジュールには、スケジュール作成者のユーザロールがあります。

View

Schedule view

定義済みユーザロール

network-admin

パラメータ

role-name: ユーザロール名を指定します。大文字、小文字を区別します。範囲は 1～63 です。ユーザロールはユーザ定義あるいは定義済みのユーザロールがあります。定義済みは network-admin、network-operator、level-0～level-15 があります。**undo user-role** コマンドで *role-name* を指定しない場合、デフォルトのユーザロールに戻します。

説明

user-role コマンドはスケジュールにユーザロールを割り当てます。

undo user-role コマンドはスケジュールからユーザロールを削除します。

スケジュールには、1 つ以上のユーザロールが必要です。スケジュール内のコマンドは、スケジュールの 1 つ以上のユーザロールによって許可されている場合に実行できます。ユーザロールの詳細については、コマンドマニュアルのセクション 1 *基本機能 “RBAC”* を参照してください。

スケジュールには最大 64 のユーザロールを設定できます。制限に達した後は、スケジュールに追加のユーザロールを割り当てることはできません。

例

ユーザロール rolename をスケジュール test に割り当てます。

<AP> system-view

[AP] scheduler schedule test

[AP-schedule-test] user-role rolename

関連コマンド

- **command**
- **scheduler**

目次

このセクションのページは **2-x-x** です。

2 章 NTP 2-1
2.1 NTP 設定コマンド 2-1
2.1.1 display ntp-service sessions 2-1
2.1.2 display ntp-service status 2-7
2.1.3 display ntp-service trace 2-10
2.1.4 ntp-service acl 2-12
2.1.5 ntp-service authentication enable 2-14
2.1.6 ntp-service authentication-keyid 2-15
2.1.7 ntp-service broadcast-client 2-17
2.1.8 ntp-service broadcast-server 2-18
2.1.9 ntp-service dscp 2-20
2.1.10 ntp-service enable 2-21
2.1.11 ntp-service inbound enable 2-22
2.1.12 ntp-service max-dynamic-sessions 2-23
2.1.13 ntp-service multicast-client 2-24
2.1.14 ntp-service multicast-server 2-26
2.1.15 ntp-service reliable authentication-keyid 2-27
2.1.16 ntp-service source 2-29
2.1.17 ntp-service unicast-peer 2-30
2.1.18 ntp-service unicast-server 2-33

2章 NTP

2.1 NTP設定コマンド

2.1.1 display ntp-service sessions

Syntax

display ntp-service sessions [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: すべての IPv4 NTP アソシエーションの詳細情報を表示します。指定しない場合、NTP アソシエーションの概要情報を表示します。

説明

display ntp-service sessions コマンドはすべての IPv4 NTP アソシエーションの情報を表示します。

装置がNTP ブロードキャストモードあるいはマルチキャストサーバモードで動作しているとき、**display ntp-service sessions** コマンドはブロードキャストサーバあるいはマルチキャストサーバに対応する IPv4 NTP アソシエーションの情報を表示しませんが、アソシエーションの総数がカウントされます。

例

すべての NTP アソシエーションの概要情報を表示します。

<AP> display ntp-service sessions

```
      source         reference      stra reach poll  now offset  delay disper
**************************************************************************
[12345]LOCAL(0)       LOCL             0     1   64    - 0.0000 0.0000 7937.9
   [5]0.0.0.0         INIT            16     0   64    - 0.0000 0.0000 0.0000
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
 Total sessions: 1
```

表 2-1 コマンド出力

フィールド	説明
source	● 参照クロックがローカルクロックであるとき、**LOCAL**(*number*)と表示されます。ローカルクロックのIPアドレスは127.127.1.*number*です。*number*はNTPプロセス番号です。値の範囲は0～3です。 ● 参照クロックが別の装置であるとき、NTPサーバのIPアドレスが表示されます。このフィールドが**0.0.0.0**である場合、NTPサーバのIPアドレスは正常に解決されていません。
reference	NTPサーバの参照クロックIDです。 ● 参照クロックがローカルクロックであるとき、straフィールドに関連した値が表示されます。 　• straフィールドの値が0あるいは1である場合、**LOCL**と表示されます。 　• straフィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。 ● 参照クロックがネットワーク上の他の装置のクロックである場合、このフィールドは装置のIPアドレスになります。装置がIPv6をサポートしている場合、装置のIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。**INIT**と表示される場合、ローカル装置はNTPサーバと接続を確立していません。
stra	クロックソースのstratumレベルです。stratumレベルはクロックの正確さを示します。値の範囲は1～16です。値が大きくなると精度が減少します。クロックの精度は1がもっとも高く、stratumが16は同期化されておらず、参照クロックを使用することができません。
reach	クロックソースの到達可能回数です。0はクロックソースが到達不能であることを示します。
poll	ポーリング間隔です。連続する2つのNTPメッセージ間の最大間隔です。
now	最後のNTPメッセージを受信、あるいはローカルクロックが最後に更新されてから現在までの時間です。 デフォルトの時間の単位は秒です。 ● 時間の長さが2048秒を超えると、分で表示されます。 ● 時間の長さが300分を超えると時間で表示されます。 ● 時間の長さが96時間を越えると日の単位で表示されます。 ● 時間の長さが999日を越えると年の単位で表示されます。

フィールド	説明
	最後のNTPメッセージを受信した時間あるいはローカルクロックが最後に更新された時間が、現在時間より遅れている場合、ハイフン（-）が表示されます。
offset	リファレンスクロックに対するシステムクロックのオフセットです。単位はミリ秒です。
delay	ローカル装置からクロックソースまでのラウンドトリップ遅延です。単位はミリ秒です。
disper	リファレンスソースに対するローカルクロックの最大誤差です。単位はミリ秒です。
[12345]	• 1—システムが選択したクロックソースです（現在のリファレンスソースです）。システムクロックstratumレベルは15以下です。 • 2—クロックソースのstratumレベルは15以下です。 • 3—クロックソースはクロック選定アルゴリズムに残りしました。 • 4—クロックソースはクロックソースの候補です。 • 5—クロックソースは設定されたコマンドで作成されました。
Total sessions	アソシエーションの総数です。

すべての IPv4 NTP アソシエーションの詳細情報を表示します。

<AP> display ntp-service sessions verbose

```
Clock source: 192.168.1.40
Session ID: 35888
Clock stratum: 2
Clock status:  configured, master, sane, valid
Reference clock ID: 127.127.1.0
Local mode: client, local poll interval: 6
Peer mode: server, peer poll interval: 6
Offset: 0.2862ms, roundtrip delay: 3.2653ms, dispersion: 4.5166ms
Root roundtrip delay: 0.0000ms, root dispersion: 10.910ms
Reachabilities:31, sync distance: 0.0194
Precision: 2^18, version: 3, source interface: Not specified
Reftime: d17cbba5.1473de1e  Tue, May 17 2011  9:17:25.079
Orgtime: 00000000.00000000  Thu, Feb  7 2036  6:28:16.000
Rcvtime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
Xmttime: d17cbbc0.b1959a30  Tue, May 17 2011  9:17:52.693
Roundtrip delay samples: 0.007 0.010 0.006 0.011 0.010 0.005 0.007 0.003
Offset samples: 5629.55 3913.76 5247.27 6526.92 31.99 148.72 38.27 0.29
```

```
Filter order: 7    5    2    6    0    4    1    3

Total sessions: 1
```

表 2-2 コマンド出力

フィールド	説明
Clock source	NTPサーバのIPアドレスです。**0.0.0.0**が表示される場合、NTPサーバのIPアドレスは正常に解決されていません。
Clock stratum	NTPサーバのstratumレベルです。stratumレベルはクロックの正確さを示します。値の範囲は1～16です。値が大きくなると精度が減少します。クロックの精度は1がもっとも高く、stratumが16は同期化されておらず、参照クロックを使用することができません。

Clock status	アソシエーションに対応するクロックソースの状態です。
	• **configured**—アソシエーションが設定コマンドで作成されました。
	• **dynamic**—ダイナミックにアソシエーションが確立されました。
	• **master**—クロックソースは現在のシステムのプライマリ参照ソースです。
	• **selected**—クロックソースはクロック選定アルゴリズムに残りました。
	• **candidate**—クロックソースはクロックソースの候補です
	• **sane**—クロックソースは認証にパスしました。参照クロックとして使用されています。
	• **insane**—クロックソースは認証に失敗しました。あるいは認証にパスしましたが参照クロックして使用されていません。
	• **valid**—クロックソースが有効です。クロックソースは以下の要件に従います。
	  • クロックソースは認証にパスし、同期しています。
	  • stratumレベルが有効です。
	  • ルート遅延とルート拡散が範囲内にあります。
	• **invalid**—クロックソースが無効です。
	• **unsynced**—クロックソースが同期されていないか、stratumレベルが無効です。

Reference clock ID	NTPサーバの参照クロックのIDです。 • 参照クロックがローカルクロックであるとき、クロックstratumフィールドに関連した値が表示されます。 • クロックstratumフィールドの値が0あるいは1である

フィールド	説明
	場合、**LOCL**と表示されます。 • クロックstratumフィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。 参照クロックがネットワーク上の他の装置のクロックである場合、このフィールドは装置のIPアドレスになります。**INIT**と表示される場合、ローカル装置はNTPサーバと接続を確立していません。
Local mode	ローカル装置の動作モードです。 • **unspec**—このモードは不特定です。 • **active**—アクティブモードです。 • **passive**—パッシブモードです。 • **client**—クライアントモードです。 • **server**—サーバモードです。 • **broadcast**—ブロードキャストあるいはマルチキャストサーバモードです。 • **bclient**—ブロードキャストあるいはマルチキャストクライアントモードです。
local poll interval	ローカル装置のポーリング間隔です。値は2の乗数で表示されます。たとえば、6が表示されている場合、ローカル装置のポーリング間隔は26あるいは64秒です。
Peer mode	ピアの装置の動作モードです。 • **unspec**—このモードは不特定です。 • **active**—アクティブモードです。 • **passive**—パッシブモードです。 • **client**—クライアントモードです。 • **server**—サーバモードです。 • **broadcast**—ブロードキャストあるいはマルチキャストサーバモードです。 • **bclient**—ブロードキャストあるいはマルチキャストクライアントモードです。
peer poll interval	ピアの装置のポーリング間隔です。値は2の乗数で表示されます。たとえば、6が表示されている場合、ローカル装置のポーリング間隔は26あるいは64秒です。
Offset	参照クロックに対するシステムクロックのオフセットです。単位はミリ秒です。
roundtrip delay	ローカル装置からクロックソースまでのラウンドトリップ遅延です。単位はミリ秒です。
dispersion	参照ソースに対するシステムクロックの最大誤差です。

フィールド	説明
Root roundtrip delay	ローカル装置からプライマリ参照ソースまでのラウンドトリップ遅延です。単位はミリ秒です。
root dispersion	プライマリ参照クロックに対するシステムクロックの最大誤差です。単位はミリ秒です。
Reachabilities	クロックソースの到達可能回数です。0は、このクロックソースが到達不可能であることを示します。
sync distance	上位レベルのクロックに対する同期距離です。単位は秒です。ばらつきとラウンドトリップ遅延の値から計算されます。
Precision	システムクロックの精度です。
version	NTPバージョンです。値の範囲は1～4です。
source interface	送信元インタフェースです。 送信元インタフェースが指定されていない場合、**Not specified**と表示されます。
Reftime	NTPメッセージの参照タイムスタンプです。
Orgtime	NTPメッセージの発生タイムスタンプです。
Rcvtime	NTPメッセージの受信タイムスタンプです。
Xmttime	NTPメッセージの送信タイムスタンプです。
Filter order	情報順序のサンプルです。
Reference clock status	ローカルクロックの状態です。このフィールドは参照クロックとしてローカルクロックを設定する**ntp-service refclock-master**コマンドを使用したときに表示されます。 ローカルクロックのreachフィールドが255であるとき、**working normally**と表示されます。そうでない場合、**working abnormally**と表示されます。
Total sessions	アソシエーションの総数です。

2.1.2 display ntp-service status

Syntax

display ntp-service status

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ntp-service status コマンドは NTP サービスの状態を表示します。

例

クロックの同期後の NTP サービスの状態を表示します。

<AP> display ntp-service status

```
Clock status: synchronized
Clock stratum: 2
System peer: LOCAL(0)
Local mode: client
Reference clock ID: 127.127.1.0
Leap indicator: 00
Clock jitter: 0.000977 s
Stability: 0.000 pps
Clock precision: 2^-10
Root delay: 0.00000 ms
Root dispersion: 3.96367 ms
Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
```

クロックを同期していないときの NTP サービスの状態を表示します。

<AP> display ntp-service status

```
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Clock jitter: 0.000000 s
Stability: 0.000 pps
Clock precision: 2^-10
Root delay: 0.00000 ms
Root dispersion: 0.00002 ms
Reference time: d0c5fc32.92c70b1e  Wed, Dec 29 2010 18:28:02.573
```

表 2-3 コマンド出力

フィールド	説明
Clock status	システムクロックの状態です。 ● **synchronized**—システムクロックが同期されています。 ● **unsynchronized**—システムクロックが同期されていません。
Clock stratum	システムクロックのstratumレベルです。
System peer	選択されたNTPサーバのIPアドレスです。
Local mode	ローカル装置の動作モードです。 ● **unspec**—このモードは不特定です。 ● **active**—アクティブモードです。 ● **passive**—パッシブモードです。 ● **client**—クライアントモードです。 ● **server**—サーバモードです。 ● **broadcast**—ブロードキャストあるいはマルチキャストサーバモードです。 ● **bclient**—ブロードキャストあるいはマルチキャストクライアントモードです。
Reference clock ID	IPv4 NTPサーバの場合、以下を示します。 ローカル装置がリモートNTPサーバに同期されているとき、このフィールドはリモートサーバのIPアドレスを表示します。 ローカル装置が参照ソースとしてローカルクロックを使用するとき、このフィールドはローカルクロックを表示します。 ● ローカルクロックのstratumフィールドの値が1である場合、**Local**と表示されます。 ● クロックstratumフィールドが別の値である場合、ローカルクロックのIPアドレスを表示します。 IPv6 NTPサーバの場合、以下を示します。 ローカル装置がリモートIPv6 NTPサーバに同期されているとき、このフィールドはリモートサーバのIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。 ローカル装置が参照ソースとしてローカルクロックを使用するとき、このフィールドはローカルクロックを表示します。 ● ローカルクロックのstratumフィールドの値が1である場合、**Local**と表示されます。 ● クロックstratumフィールドが別の値である場合、ローカ

フィールド	説明
	ルクロックのIPv6アドレスの最初の32ビットのMD5ダイジェストを表示します。
Leap indicator	アラーム状態です。 ● **00**—正常です。 ● **01**—leap秒です。一日の最後の分が61秒であることを示します。 ● **10**— leap秒です。一日の最後の分が59秒であることを示します。 ● **11**—クロックが同期されていません。
Clock jitter	システムクロックと参照クロック間の相違です。単位は秒です。
Stability	クロック周波数の安定性です。値が低い場合、安定性が高いことを示します。
Clock precision	システムクロックの精度です。
Root delay	ローカル装置からプライマリ参照ソースまでのラウンドトリップ遅延です。単位はミリ秒です。
Root dispersion	プライマリ参照クロックに対するシステムクロックの最大誤差です。単位はミリ秒です。
Reference time	参照タイムスタンプです。

2.1.3 display ntp-service trace

Syntax

display ntp-service trace [**source** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

source *interface-type interface-number:* NTP パケットを送信して、ローカルデバイスからプライマリ参照ソースまで各NTP サーバを追跡するための送信元インタフェースを指定します。NTP パケットの送信元 IP アドレスは、指定された送信元インタフェースの IPv 4 アドレスです。NTP サーバの IP アドレスがリンクローカルアドレスの場合、NTP パケットの発信インタフェースのリンクローカルアドレスが NTP パケットの送信元 IP アドレスとして使用されます。このオプションを指定しない場合、追跡した NTP パケットを送信するインタフェースが送信元インタフェースとして機能します。

説明

display ntp-service trace コマンドはローカル装置からプライマリ参照ソース間の NTP サーバの概要情報を表示します。

例

ローカル装置からプライマリ参照ソース間の NTP サーバの概要情報を表示します。

<AP> display ntp-service trace

```
Server    127.0.0.1
Stratum   3, jitter  0.000, synch distance 0.0000.
Server    3000::32
Stratum   2 , jitter 790.00, synch distance 0.0000.
RefID     127.127.1.0
```

出力は、サーバ 127.0.0.1 がサーバ 3000::32 に同期しており、サーバ 3000::32 がローカルクロックに同期していることを示します。

表 2-4 コマンド出力

フィールド	説明
Server	NTPサーバのIPアドレスです。

フィールド	説明
Stratum	NTPサーバのstratumレベルです。
jitter	上位レベルクロックに対するクロックオフセットのRMS（Root mean square）です。単位は秒です。
synch distance	上位レベルのNTPサーバに対する同期間隔です。単位は秒です。ばらつきとラウンドトリップ遅延の値から計算されます。
RefID	プライマリ参照ソースの識別子です。プライマリ参照クロックのstratumレベルが0であるとき、**Local**と表示されます。そうでなければプライマリ参照クロックのIPアドレスが表示されます。

関連コマンド

- **ntp-service source**
- **ntp-service unicast-server**
- **ntp-service unicast-peer**

2.1.4 ntp-service acl

Syntax

ntp-service { **peer** | **query** | **server** | **synchronization** } **acl** *ipv4-acl-number*

undo ntp-service { **peer** | **query** | **server** | **synchronization** } [**acl** *ipv4-acl-number*]

デフォルト

peer

View

System view

定義済みユーザロール

network-admin

パラメータ

peer: タイム要求とピア装置からの NTP 制御クエリ（アラーム、認証状態、タイムサーバ情報など）を許可します。ローカル装置がピアの装置と同期することを許可します。

query: ピア装置からローカル装置の NTP 制御クエリのみ許可します。

server: タイム要求とピア装置からの NTP 制御クエリを許可します。ローカル装置がピアの装置と同期することを許可しません。

synchronization: ACL にパスするアドレスのシステムからのタイム要求のみ許可します。

acl *ipv4-acl-number*: IPv4 ACL を指定します。ACL に一致するピアの装置は NTP サービスアクセス制御権があります。*ipv4-acl-number* は ACL 番号を示します。標準 IPv4 ACL の設定範囲は 2000～2999 です。拡張 IPv4 ACL の設定範囲は 3000～3999 です。

説明

ntp-service acl コマンドはローカル装置の IPv4 NTP サービスにアクセスするため、ピアの NTP サービスアクセス制御権を設定します。

undo ntp-service acl コマンドは IPv4 NTP サービスの NTP サービスアクセス制御権を削除します。

IPv4 ACL 要求によって NTP アクセスを制御することができます。**peer**、**server**、**synchronization**、**query** の順番でアクセス制御権の制限が高くなります。

装置は以下のルールで IPv4 NTP 要求を処理します。

- IPv4 NTP サービスアクセス制御権が設定されていない場合、**peer** はローカル装置とピアの装置に与えられます。
- ピアの装置の IP アドレスが複数のアクセス制御権のため IPv4 ACL の **permit** 条件に一致する場合、もっとも制限のないアクセス制御権がピアの装置に与えられます。**deny** 条件あるいは IPv4 ACL に一致しない場合、アクセス制御権は与えられません。

- アクセス制御権の IPv4 ACL が作成されていない場合、関連するアクセス制御権は与えられません。
- すべてのアクセス制御権の IPv4 ACL が作成されていない場合、**peer** が与えられます。
- すべてのアクセス制御権の IPv4 ACL がルールに含まれていない場合、アクセス制御権は与えられません。

ntp-service acl コマンドは NTP が動作するシステムで最低限のセキュリティを提供します。より安全な方法は NTP 認証です。

例

サブネット 10.10.0.0/16 のピアの装置がローカル装置にフルアクセスできるように設定します。

<AP> system-view

[AP] acl basic 2001

[AP-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255

[AP-acl-ipv4-basic-2001] quit

[AP] ntp-service peer acl 2001

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

2.1.5 ntp-service authentication enable

Syntax

ntp-service authentication enable

undo ntp-service authentication enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ntp-service authentication enable コマンドは NTP 認証を有効にします。

undo ntp-service authentication enable コマンドは NTP 認証を無効にします。

認証された NTP サーバに NTP クライアントが同期できるように、クロック同期のセキュリティが必要なネットワークで NTP 認証を有効にしてください。

NTP サーバを認証するため、認証キーを設定し、トラステッドキーとして指定します。

例

NTP 認証を有効にします。

<AP> system-view

[AP] ntp-service authentication enable

関連コマンド

- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

2.1.6 ntp-service authentication-keyid

Syntax

ntp-service authentication-keyid *keyid* **authentication-mode md5** { **cipher** | **simple** } *string* [**acl** *ipv4-acl-number*] *

undo ntp-service authentication-keyid *keyid*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid: 認証キーを識別するため、キーID を指定します。設定範囲は 1～4294967295 です。

authentication-mode: 認証アルゴリズムを指定します。

md5: 認証に MD5 アルゴリズムを使用します。

cipher: 暗号テキスト認証キーを設定します。

simple: プレーンテキスト認証キーを設定します。セキュリティのためプレーンテキストで設定された認証キーを含むすべての認証キーは暗号テキストで保存されます。

string: 認証キーを指定します。大文字、小文字を区別します。プレーンテキスト認証キーの設定範囲は 1～32 文字です。暗号テキスト認証キーの設定範囲は 1～73 文字です。

acl *ipv4-acl-number:* IPv4 ACL を指定します。ACL で許可されたデバイスのみが認証にキーID を使用できます。標準 IPv4 ACL の設定範囲は 2000～2999 です。

説明

ntp-service authentication-keyid コマンドは NTP 認証キーを設定します。

undo ntp-service authentication-keyid コマンドは NTP 認証キーを削除します。

時刻同期セキュリティを必要とする NTP ネットワークでは、NTP 認証を有効にする必要があります。NTP 認証により、NTP クライアントは認証された NTP タイムサーバに対してのみ同期されます。ピアの装置からのメッセージ内のキーID は、認証に使用されるキーを識別します。**acl** *ipv4-acl-number* オプションは、キーID を使用できるピアの装置を識別するために使用されます。

- 装置は、**acl** *ipv4-acl-number* オプションを使用してピアの装置への NTP セッションが確立されるか、またはすでに存在している場合にのみ、ピアの装置がキーID を使用できるかどうか識別します。

- 指定した ACL が存在しない場合、または指定した ACL にルールが含まれていない場合は、どの装置でも認証にキーID を使用できます。

NTP 認証を成功させるには、タイムサーバとクライアントで同じキーID とキーを設定します。ピアの装置がローカルデバイスでの認証にキーID を使用できることを確認します。

NTP 認証キーを指定した後、トラステッドキーとして設定するため **ntp-service reliable authentication-keyid** コマンドを使用します。キーを削除した後、キーは自動で非トラステッドキーに変更します。この場合、**undo ntp-service reliable authentication-keyid** コマンドを実行する必要はありません。

このコマンドを使用して最大 128 のキーを設定することができます。

例

キーの ID が 10、キーの値が **BetterKey** のプレーンテキスト MD5 認証キーを設定します。

<AP> system-view

[AP] ntp-service authentication enable

[AP] ntp-service authentication-keyid 10 authentication-mode md5 simple BetterKey

関連コマンド

- **ntp-service authentication enable**
- **ntp-service reliable authentication-keyid**

2.1.7 ntp-service broadcast-client

Syntax

ntp-service broadcast-client

undo ntp-service broadcast-client

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service broadcast-client コマンドは NTP ブロードキャストクライアントモードで動作するように設定し、現在のインタフェースで NTP ブロードキャストパケットを受信します。

undo ntp-service broadcast-client コマンドは設定を削除します。

コマンドを設定した後、装置は NTP ブロードキャストが送信した NTP メッセージを受信し、受信した NTP メッセージをもとに同期します。

このコマンドによって、装置のインタフェースがブロードキャストクライアントモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP ブロードキャストクライアントモードで動作するように設定し、VLAN インタフェース 1 で NTP ブロードキャストパケットを受信します。

<AP> system-view

[AP] interface vlan-interface 1

[AP-Vlan-interface1] ntp-service broadcast-client

関連コマンド

ntp-service broadcast-server

2.1.8 ntp-service broadcast-server

Syntax

ntp-service broadcast-server [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

authentication-keyid *keyid*: ブロードキャストメッセージをクライアントに送信するために使用するキーID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置は NTP 認証が有効のブロードキャストクライアントを同期できません。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service broadcast-server コマンドは NTP ブロードキャストサーバモードで動作するように設定し、現在のインタフェースで NTP ブロードキャストパケットを送信します。

undo ntp-service broadcast-server コマンドは設定を削除します。

コマンドを設定した後、装置は定期的に NTP メッセージをブロードキャストアドレス 255.255.255.255 に送信します。

このコマンドによって、装置のインタフェースがブロードキャストサーバモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP ブロードキャストサーバモードで動作するように設定し、VLAN インタフェース 1 で暗号キーID が 4、NTP のバージョンが 4 の NTP ブロードキャストメッセージを送信します。

<AP> system-view

[AP] interface vlan-interface 1

[AP-Vlan-interface1] ntp-service broadcast-server authentication-keyid 4 version 4

関連コマンド

ntp-service broadcast-client

2.1.9 ntp-service dscp

Syntax

ntp-service dscp *dscp-value*

undo ntp-service dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: IPv4 NTP パケットの DSCP を設定します。設定範囲は 0〜63 です。

説明

ntp-server dscp コマンドは IPv4 NTP パケットの DSCP を設定します。

undo ntp-server dscp コマンドはデフォルトに戻します。

パケットの優先度を識別するため、DSCP は IPv4 パケットの ToS フィールドに含まれます。

例

IPv4 NTP パケットの DSCP を 30 に設定します。

<AP> system-view

[AP] ntp-service dscp 30

2.1.10 ntp-service enable

Syntax

ntp-service enable

undo ntp-service enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ntp-service enable コマンドは NTP サービスを有効にします。

undo ntp-service enable コマンドは NTP サービスを無効にします。

例

NTP サービスを有効にします。

<AP> system-view

[AP] ntp-service enable

2.1.11 ntp-service inbound enable

Syntax

ntp-service inbound enable

undo ntp-service inbound enable

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

ntp-service inbound enableコマンドはインタフェースでNTPメッセージの処理を有効にします。

undo ntp-service inbound enable コマンドはデフォルトに戻します。

以下の場合、インタフェースで **undo ntp-service inbound enable** コマンドを実行してください。

- 装置のインタフェースが対応するサブネットで、ピアの装置と同期しません。
- 装置がインタフェースと一致しているサブネットでピアの装置によって同期しません。

例

VLAN インタフェース 1 で NTP メッセージの処理を無効にします。

<AP> system-view

[AP] interface vlan-interface 1

[AP-Vlan-interface1] undo ntp-service inbound enable

2.1.12 ntp-service max-dynamic-sessions

Syntax

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

デフォルト

100

View

System view

定義済みユーザロール

network-admin

パラメータ

number: ダイナミック NTP アソシエーションの最大数を設定します。設定範囲は 0～100 です。

説明

ntp-service max-dynamic-sessions コマンドはダイナミック NTP アソシエーションの最大数を設定します。

undo ntp-service max-dynamic-sessions コマンドはデフォルトに戻します。

装置はスタティックアソシエーションとダイナミックアソシエーションを含めて共通で最大 128 のアソシエーションを設定することができます。スタティックアソシエーションは NTP コマンドを使用して手動で作成されたユーザのアソシエーションを参照します。ダイナミックアソシエーションはシステムの動作中に一時的に作成されたアソシエーションです。

ntp-service max-dynamic-sessions コマンドは、ダイナミックアソシエーションが多くのシステムリソースを占有しないように制限させるため、ダイナミックアソシエーションの最大数を制限します。

例

ダイナミック NTP アソシエーションの最大数を 50 に設定します。

<AP> system-view

[AP] ntp-service max-dynamic-sessions 50

関連コマンド

display ntp-service sessions

2.1.13 ntp-service multicast-client

Syntax

ntp-service multicast-client [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: マルチキャスト IP アドレスを指定します。デフォルトは 224.0.1.1 です。マルチキャストサーバとクライアントは同一のマルチキャスト IP アドレスに設定する必要があります。

説明

ntp-service multicast-client コマンドは NTP マルチキャストクライアントモードで動作するように設定し、現在のインタフェースで NTP マルチキャストパケットを受信します。

undo ntp-service multicast-client コマンドは設定を削除します。

コマンドを設定した後、装置は宛先アドレスとして指定したマルチキャストアドレスを使用し NTP メッセージを受信します。

このコマンドによって、装置のインタフェースがマルチキャストクライアントモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP マルチキャストクライアントモードで動作するように設定します。VLAN インタフェース 1 で NTP マルチキャストパケットを受信し、マルチキャストアドレスを 224.0.1.1 に設定します。

<AP> system-view

[AP] interface vlan-interface 1

[AP-Vlan-interface1] ntp-service multicast-client 224.0.1.1

関連コマンド

ntp-service multicast-server

2.1.14 ntp-service multicast-server

Syntax

ntp-service multicast-server [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

デフォルト

装置は NTP アソシエーションモードで動作しません。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: マルチキャスト IP アドレスを指定します。デフォルトは 224.0.1.1 です。マルチキャストサーバとクライアントは同一のマルチキャスト IP アドレスに設定する必要があります。

authentication-keyid *keyid*: マルチキャストメッセージをクライアントに送信するために使用するキーID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置は NTP 認証が有効のマルチキャストクライアントを同期できません。

ttl *ttl-number*: NTP マルチキャストメッセージの TTL を指定します。設定範囲は 1～255 です。デフォルトは 16 です。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service multicast-server コマンドは NTP マルチキャストサーバモードで動作するように設定し、現在のインタフェースで NTP マルチキャストパケットを送信します。

undo ntp-service multicast-server コマンドは設定を削除します。

コマンドを設定した後、装置は定期的に NTP メッセージをマルチキャストアドレスに送信します。

このコマンドによって、装置のインタフェースがマルチキャストサーバモードで動作するように設定されている場合、アグリゲーショングループにインタフェースを追加することができません。アグリゲーショングループにインタフェースを追加する場合、コマンドの設定を削除してください。

例

NTP マルチキャストサーバモードで動作するように設定し、VLAN インタフェース 1 で暗号キーID が 4、NTP のバージョンが 4 の NTP マルチキャストメッセージをマルチキャストアドレス 224.0.1.1 に送信します。

<AP> system-view

[AP] interface vlan-interface 1

[AP-Vlan-interface1] ntp-service multicast-server 224.0.1.1 version 4 authentication-keyid 4

関連コマンド

ntp-service multicast-client

2.1.15 ntp-service reliable authentication-keyid

Syntax

ntp-service reliable authentication-keyid *keyid*

undo ntp-service reliable authentication-keyid *keyid*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyid: 認証キーを指定します。設定範囲は 1～4294967295 です。

説明

ntp-service reliable authentication-keyid コマンドは作成された認証キーをトラステッドキーとして指定します。

undo ntp-service reliable authentication-keyid コマンドは設定を削除します。

NTP 認証が有効であるとき、クライアントは信頼された認証キーを提供するサーバにのみ同期することができます。

このコマンドを使用する前に、NTP 認証が有効で認証キーが設定されていることを確認してください。キーを削除した後、キーは自動で非トラステッドキーに変更します。こ

の場合、**undo ntp-service reliable authentication-keyid** コマンドを実行する必要はありません。

例

NTP 認証を有効にし、キーの ID が 37、キーの値が **BetterKey** の MD5 アルゴリズムの認証キーを設定します。

<AP> system-view

[AP] ntp-service authentication enable

[AP] ntp-service authentication-keyid 37 authentication-mode md5 simple BetterKey

トラステッドキーとして指定します。

[AP] ntp-service reliable authentication-keyid 37

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**

2.1.16 ntp-service source

Syntax

ntp-service source *interface-type interface-number*

undo ntp-service source

デフォルト

NTP メッセージのインタフェースは指定されていません。装置は以下の処理を行います。

- NTP メッセージの送信インタフェースをルーティングテーブルから検索します。
- NTP メッセージの送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

ntp-service source コマンドは NTP メッセージの送信元インタフェースを指定します。

undo ntp-service source コマンドはデフォルトに戻します。

NTP メッセージの送信元インタフェースを指定する場合、装置は NTP メッセージを送信するとき、指定されたインタフェースのプライマリ IP アドレスとして NTP メッセージの送信元 IP アドレスを設定します。

装置が NTP 要求に応答するとき、NTP 応答の送信元 IP アドレスは常に NTP 要求を受信したインタフェースの IP アドレスです。

応答メッセージの宛先アドレスにローカル装置のインタフェースの IP アドレスを使用しない場合、NTP メッセージの送信元インタフェースとして別のインタフェースを指定するため **ntp-service source** コマンドを使用します。

NTP メッセージの送信元インタフェースは以下の方法で指定することができます。

- NTP クライアント/サーバモードでは、**ntp-service unicast-server** コマンドで、NTP メッセージの送信元インタフェースを指定した場合、**ntp-service unicast-server** コマンドで指定したインタフェースは NTP メッセージの送信元インタフェースとして動作します。
- NTP シンメトリックアクティブ/パッシブモードでは、**ntp-service unicast-peer** コマンドで、NTP メッセージの送信元インタフェースを指定した場合、**ntp-service**

unicast-peer コマンドで指定したインタフェースは NTP メッセージの送信元インタフェースとして動作します。

- NTP マルチキャストモードでは、**ntp-service multicast-server** コマンドが設定された場合、マルチキャスト NTP メッセージの送信元インタフェースは、NTP マルチキャストメッセージの送信元インタフェースとして動作します。
- NTP ブロードキャストモードでは、**ntp-service broadcast-server** コマンドが設定された場合、ブロードキャスト NTP メッセージの送信元インタフェースは、NTP ブロードキャストメッセージの送信元インタフェースとして動作します。

指定した送信元インタフェースが down している場合、装置は NTP メッセージを送信しません。

例

NTP メッセージの送信元インタフェースとして VLAN インタフェース 1 を指定します。

<AP> system-view

[AP] ntp-service source vlan-interface 1

2.1.17 ntp-service unicast-peer

Syntax

ntp-service unicast-peer { *peer-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer { *peer-name* | *ip-address* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

peer-name: シンメトリックーパッシブピアのホスト名を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

ip-address: シンメトリックーパッシブピアの IP アドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルクロックの IP アドレスでなくユニキャストアドレスにする必要があります。

authentication-keyid *keyid*: NTP メッセージをピアに送信するために使用するキーの ID を指定します。設定範囲は 1～4294967295 です。指定しない場合、ローカル装置とピアは互いに認証しません。

maxpoll *maxpoll-interval:* 最大ポーリング間隔を指定します。*maxpoll-interval* 引数の値の設定範囲は 4～17 です。最大ポーリング間隔は、これに基数 2 を上げて間隔を秒単位で取得します。最大ポーリング間隔は 2^4 ～ 2^{17} (16 ～ 131072) 秒の範囲です。*maxpoll-interval* 引数の値のデフォルト値は 6 で、デフォルトの最大ポーリング間隔は 2^6 (64) 秒です。

minpoll *minpoll-interval:* 最小ポーリング間隔を指定します。*minpoll-interval* 引数の値の設定範囲は 4～17 です。最小ポーリング間隔は、これに基数 2 を上げて間隔を秒単位で取得します。最小ポーリング間隔は、2^4 から 2^{17} (16 から 131072) 秒の範囲です。*minpoll-interval* 引数のデフォルト値は 6 で、デフォルトの最小ポーリング間隔は 26 (64) 秒です。

priority: 同一条件のもとで最初の選択として、*ip-address* あるいは *peer-name* で指定されたピアを指定します。

source *interface-type interface-number*: NTP メッセージの送信元インタフェースを指定します。ローカル装置がピアに NTP メッセージを送信する場合、送信元 IP アドレスはインタフェースのプライマリ IP アドレスです。*interface-type interface-number* はインタフェースのタイプと番号を示します。指定しない場合、出力インタフェースをルーティングテーブルから検索し、NTP メッセージの送信元 IP アドレスとして出力インタフェースのプライマリ IP アドレスを使用します。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service unicast-peer コマンドは装置のシンメトリックーパッシブピアを指定します。

undo ntp-service unicast-peer コマンドは装置の指定されたシンメトリックーパッシブピアを削除します。

装置のパッシブピアを指定するとき、装置と装置のパッシブピアは互いに同期することができます。クロックが同期されている場合、高い stratum レベルのクロックは、低い stratum レベルのクロックに同期されます。

例

装置のシンメトリックーパッシブピアとして IP アドレス 10.1.1.1 の装置を指定します。NTP バージョンを 4、NTP メッセージの送信元インタフェースを VLAN インタフェース 1 に設定します。

<AP> system-view

[AP] ntp-service unicast-peer 10.1.1.1 version 4 source-interface vlan-interface 1

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

2.1.18 ntp-service unicast-server

Syntax

ntp-service unicast-server { *server-name* | *ip-address* } [**authentication-keyid** *keyid* | **maxpoll** *maxpoll-interval* | **minpoll** *minpoll-interval* | **priority** | **source** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server { *server-name* | *ip-address* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

server-name: NTP サーバのホスト名を指定します。設定範囲は 1〜253 文字です。大文字、小文字を区別しません。

ip-address: NTP サーバの IP アドレスを指定します。ブロードキャストアドレス、マルチキャストアドレス、ローカルクロックの IP アドレスでなくユニキャストアドレスにする必要があります。

authentication-keyid *keyid*: NTP メッセージを NTP サーバに送信するために使用するキーの ID を指定します。設定範囲は 1〜4294967295 です。指定しない場合、ローカル装置と NTP サーバは互いに認証しません。

maxpoll *maxpoll-interval:* 最大ポーリング間隔を指定します。*maxpoll-interval* 引数の値の設定範囲は 4〜17 です。最大ポーリング間隔は、これに基数 2 を上げて間隔を秒単位で取得します。最大ポーリング間隔は 2^4 〜 2^{17} (16 〜 131072) 秒の範囲です。*maxpoll-interval* 引数の値のデフォルト値は 6 で、デフォルトの最大ポーリング間隔は 2^6 (64) 秒です。

minpoll *minpoll-interval:* 最小ポーリング間隔を指定します。*minpoll-interval* 引数の値の設定範囲は 4〜17 です。最小ポーリング間隔は、これに基数 2 を上げて間隔を秒単位で取得します。最小ポーリング間隔は、2^4 から 2^{17} (16 から 131072) 秒の範囲です。*minpoll-interval* 引数のデフォルト値は 6 で、デフォルトの最小ポーリング間隔は 26 (64) 秒です。

priority: 同一条件のもとで最初の選択として、NTP サーバを指定します。

source *interface-type interface-number*: NTP メッセージの送信元インタフェースを指定します。ローカル装置が NTP サーバに NTP メッセージを送信する場合、送信元 IP アドレスはインタフェースのプライマリ IP アドレスです。*interface-type interface-number* は

インタフェースのタイプと番号を示します。指定しない場合、出力インタフェースをルーティングテーブルから検索し、NTP メッセージの送信元 IP アドレスとして出力インタフェースのプライマリ IP アドレスを使用します。

version *number*: NTP バージョンを指定します。設定範囲は 1～4 です。デフォルトは 4 です。

説明

ntp-service unicast-server コマンドは装置の NTP サーバを指定します。

undo ntp-service unicast-server コマンドは装置から指定された NTP サーバを削除します。

装置の NTP サーバを指定するとき、装置は NTP サーバに同期されますが、NTP サーバは装置に同期されません。

例

装置の NTP サーバ 10.1.1.1 を指定します。NTP バージョンを 4 で動作するように装置を設定します。

<AP> system-view

[AP] ntp-service unicast-server 10.1.1.1 version 4

関連コマンド

- **ntp-service authentication enable**
- **ntp-service authentication-keyid**
- **ntp-service reliable authentication-keyid**

目次

このセクションのページは **2-x-x** です。

3 章 Information Center 3-1
3.1 Information Center 設定コマンド 3-1
3.1.1 display info-center 3-1
3.1.2 display logbuffer 3-2
3.1.3 display logbuffer summary 3-4
3.1.4 enable log updown 3-5
3.1.5 info-center enable 3-6
3.1.6 info-center logbuffer 3-6
3.1.7 info-center logbuffer size 3-7
3.1.8 info-center loghost 3-8
3.1.9 info-center loghost source 3-9
3.1.10 info-center source 3-11
3.1.11 info-center synchronous 3-13
3.1.12 info-center syslog min-age 3-15
3.1.13 info-center timestamp 3-15
3.1.14 info-center timestamp loghost 3-17
3.1.15 reset logbuffer 3-18
3.1.16 terminal debugging 3-19
3.1.17 terminal logging level 3-20
3.1.18 terminal monitor 3-21

3章 Information Center

3.1 Information Center設定コマンド

3.1.1 display info-center

Syntax

display info-center

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display info-center コマンドは Information Center の情報を表示します。

例

Information Center の情報を表示します。

<AP> display info-center

```
Information Center: Enabled
Console: Enabled
Monitor: Enabled
Log host: Enabled
   192.168.0.1,
   port number: 5000, host facility: local7
Log buffer: Enabled
   Max buffer size 1024, current buffer size 512,
   Current messages 0, dropped messages 0, overwritten messages 0
Log file: Enabled
Security log file: Enabled
Information timestamp format:
   Log host: Date
   Other output destination: Date
```

3.1.2 display logbuffer

Syntax

display logbuffer [**reverse**] [**level** *severity* | **size** *buffersize*] * [**last-mins** *mins*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

reverse: 最新のログエントリを年代順で上から表示します。指定しない場合、もっとも古いログエントリを上から表示します。

level *severity*: severity レベルを指定します。設定範囲は 0～7 です。指定しない場合、すべてのレベルのログ情報を表示します。

表 3-1 ログレベル

Severity	レベル	説明	コマンドに対応するキーワード
0	Emergency	システムが使用できません。たとえば、システムの許可が終了しました。	emergency
1	Alert	即急に対応が必要です。たとえば、インタフェースのトラフィックが上限を超えました。	alert
2	Critical	深刻な状態です。たとえば、装置の温度が上限を超えました、電源モジュールが故障しました、FANトレイが故障しました。	critical
3	Error	エラー状態です。たとえば、リンク状態が変更しました。	error
4	Warning	警告状態です。たとえば、インタフェースが切断されました、あるいはメモリリソースが上限まで使われました。	warning
5	Notification	通常通りですが、注意状態です。たとえば、装置にログインしました、あるいは装置が再起動しました。	notification
6	Informational	情報メッセージです。たとえば、コマンドあるいは**ping**コマンドが実行されました。	informational
7	Debugging	デバッグメッセージです。	debugging

size *buffersize*: 表示される最新のログメッセージの数を指定します。設定範囲は 1～1024 です。指定しない場合、すべてのログ情報を表示します。

last-mins *mins:* 最後に指定した期間にバッファされたログを表示します。mins 引数は、1~43200 分の範囲で期間を指定します。期間を指定しない場合、コマンドはログバッファ内のすべてのログを表示します。

説明

display logbuffer コマンドはログバッファの状態とログバッファのログ情報を表示します。

例

ログバッファの状態とログ情報を表示します。

<AP> display logbuffer

```
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 718
Current messages: 512
%Jun 17 15:57:09:578 2016 AP SYSLOG/7/SYS_RESTART:System restarted --
...
```

ログバッファ情報と過去 5 分間にバッファされたログを表示します。

<AP>display logbuffer last-mins 5

```
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 512
Dropped messages: 0
Overwritten messages: 0
Current messages: 191
%Jan 1 01:00:06:784 2018 Sysname SHELL/6/SHELL_CMD:
-Line=vty0-IPAddr=192.168.1.242-User=**;Command is display
current-configuration
%Jan 1 01:03:19:691 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from
192.168.1.33.
```

表 3-2 コマンド出力

フィールド	説明
Log buffer	• **Enabled**—ログバッファにログを出力できます。 • **Disabled**—ログバッファにログを出力できません。
Max buffer size	装置でサポートしている最大バッファサイズです。

フィールド	説明
Actual buffer size	**info-center logbuffer size**コマンドで設定された最大バッファサイズです。
Dropped messages	廃棄されたメッセージ数です。
Overwritten messages	上書きされたメッセージ数です。
Current messages	現在のメッセージ数です。
Failed to obtain the specified data. The following tries to display all data in the log buffer	指定されたデータの取得に失敗しました。システムはログバッファ内のすべてのデータを表示しようとします。

関連コマンド

- **info-center logbuffer**
- **reset logbuffer**

3.1.3 display logbuffer summary

Syntax

display logbuffer summary [**level** *severity*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

level *severity*: severity レベルを指定します。設定範囲は 0～7 です。指定しない場合、すべてのレベルのログ情報を表示します。ログレベルの詳細は表 3-1 を参照してください。

説明

display logbuffer summary コマンドはログバッファの概要を表示します。

例

ログバッファの概要を表示します。

<AP> display logbuffer summary

```
  EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
```

0 0 0 7 0 34 38 0

表 3-3 コマンド出力

フィールド	説明
EMERG	emergencyを示します。詳細は表 3-14を参照してください。
ALERT	alertを示します。詳細は表 3-14を参照してください。
CRIT	criticalを示します。詳細は表 3-14を参照してください。
ERROR	errorを示します。詳細は表 3-14を参照してください。
WARN	warningを示します。詳細は表 3-14を参照してください。
NOTIF	notificationを示します。詳細は表 3-14を参照してください。
INFO	informationalを示します。詳細は表 3-14を参照してください。
DEBUG	debugを示します。詳細は表 3-14を参照してください。

3.1.4 enable log updown

Syntax

enable log updown

undo enable log updown

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

enable log updown コマンドはインタフェースの状態が変化したとき、インタフェースでリンクアップあるいはリンクダウンのログを作成することを有効にします。

undo enable log updown コマンドはインタフェースの状態が変化したとき、インタフェースでリンクアップあるいはリンクダウンのログを作成することを無効にします。

例

GigabitEthernet1/0/1 でリンクアップあるいはリンクダウンのログを作成することを無効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] undo enable log updown

3.1.5 info-center enable

Syntax

info-center enable

undo info-center enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center enable コマンドは Information Center を有効にします。

undo info-center enable コマンドは Information Center を無効にします。

例

Information Center を有効にします。

<AP> system-view

[AP] info-center enable

```
Information center is enabled.
```

3.1.6 info-center logbuffer

Syntax

info-center logbuffer

undo info-center logbuffer

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

info-center logbuffer コマンドはログバッファにログの出力を有効にします。

undo info-center logbuffer コマンドはログバッファにログの出力を無効にします。

例

ログバッファにログ情報を出力するように設定します。

<AP> system-view

[AP] info-center logbuffer

関連コマンド

- **display logbuffer**
- **info-center enable**

3.1.7 info-center logbuffer size

Syntax

info-center logbuffer size *buffersize*

undo info-center logbuffer size

デフォルト

512

View

System view

定義済みユーザロール

network-admin

パラメータ

buffersize: ログバッファに記憶できるログの最大数を指定します。設定範囲は 0～1024 です。デフォルトは 512 です。

説明

info-center logbuffer size コマンドはログバッファに記憶できるログの最大数を設定します。

undo info-center logbuffer size コマンドはデフォルトに戻します。

例

ログバッファに記憶できるログの最大数を 50 に設定します。

<AP> system-view

[AP] info-center logbuffer size 50

ログのバッファサイズをデフォルトに戻します。

<AP> system-view

[AP] undo info-center logbuffer size

関連コマンド

- **display logbuffer**
- **info-center enable**

3.1.8 info-center loghost

Syntax

info-center loghost { *hostname* | *ipv4-address* } [**port** *port-number*] [**facility** *local-number* | **filter** *filter-name* | **format** { **default** | **rfc5424** | **unicom** } | **port** *port-number* | **source-ip** *source-ip-address*] *

undo info-center loghost { *hostname* | *ipv4-address* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

hostname: ログホスト名を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

ipv4-address: ログホストの IPv4 アドレスを指定します。

port *port-number*: ログホストのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 514 です。設定された値はログホストで設定された値と同じにする必要があります。そうでない場合、ログホストはシステム情報を受信できません。

facility *local-number*: ログホストのロギング facility を指定します。設定範囲は local0～local7 です。デフォルトは local7 です。ロギング facility は異なるロギングの送信元、query、ログのフィルタリングを識別するために使用します。

filter *filter-name*: ログホストへのログ出力を制御するログ出力フィルタを指定します。*filter-name* 引数は、フィルタ名 (大文字と小文字を区別しない 1~8 文字の文字列) を表し

ます。ログ出力フィルタを指定しない場合は、ログホストの宛先に対して **info-center source** コマンドを使用して設定したログ出力ルールが使用されます。

Format { **default** | **rfc 5424** | **unicom**}: ログホストに送信するログの形式を指定します。

このキーワードを指定しない場合は、**info-center format** コマンドで指定した形式が使用されます。

- **default**: カスタマイズされていない形式を指定します。
- **rfc 5424**: RFC 5424 形式を指定します。
- **unicom**: Unicom 形式を指定します。

説明

info-center loghost コマンドはログホストを指定し、出力パラメータを設定します。

undo info-center loghost コマンドはデフォルトに戻します。

info-center enable コマンドで有効にしたのち、**info-center loghost** コマンドは適用されます。

例

ログホスト 1.1.1.1 にログを出力します。

<AP> system-view

[AP] info-center loghost 1.1.1.1

3.1.9 info-center loghost source

Syntax

info-center loghost source *interface-type interface-number*

undo info-center loghost source

デフォルト

出力ログの送信元 IP アドレスは、ルートの送信インタフェースに一致するプライマリ IP アドレスです。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: ログの送信インタフェースのタイプと番号を指定します。

説明

info-center loghost source コマンドは出力ログの送信元 IP アドレスを指定します。

undo info-center loghost source コマンドはデフォルトに戻します。

ログを出力するため物理インタフェースが使用されても、システムはログ情報の送信元 IP アドレスとして指定された送信インタフェースのプライマリ IP アドレスを使います。

info-center enable コマンドで有効にしたのち、**info-center loghost source** コマンドは適用されます。

例

出力ログの送信元 IP アドレスとしてループバック 0 の IP アドレスを指定します。

<AP> system-view

[AP] interface loopback 0

[AP-LoopBack0] ip address 2.2.2.2 32

[AP-LoopBack0] quit

[AP] info-center loghost source loopback 0

関連コマンド

info-center loghost

3.1.10 info-center source

Syntax

info-center source { *module-name* | **default** } { **console** | **logbuffer** | **loghost** | **monitor** } { **deny** | **level** *severity* }

undo info-center source { *module-name* | **default** } { **console** | **logbuffer** | **loghost** | **monitor** }

デフォルト

表 3-4 にデフォルトのログ出力ルールを示します。

表 3-4 デフォルト出力ルール

宛先	送信元モジュール	共通ログ	Hidden ログ
コンソール	サポートされるすべてのモジュールです。	debugging	無効
モニタ端末	サポートされるすべてのモジュールです。	debugging	無効
ログホスト	サポートされるすべてのモジュールです。	informational	informational
ログバッファ	サポートされるすべてのモジュールです。	informational	informational

View

System view

定義済みユーザロール

network-admin

パラメータ

module-name: モジュールの名前を指定します。たとえば、FTP の情報を出力する場合、FTP を指定します。装置でサポートされているモジュールを表示する場合、使用します。

default: すべてのモジュールを指定します。装置でサポートされているモジュールを表示する場合、**info-center source ?**コマンドを使用します。

console: コンソールにログを出力します。

logbuffer: ログバッファにログを出力します。

loghost: ログホストにログを出力します。

monitor: モニタ端末にログを出力します。

deny: ログの出力を無効にします。

level *severity*: severity レベルを指定します。設定範囲は 0～7 です。詳細は表 3-1 を参照してください。出力を許可/拒否されたログのもっとも低い severity レベルを指定することができます。

説明

info-center source コマンドはモジュールのログの出力ルールを設定します。

undo info-center source コマンドはデフォルトに戻します。

モジュールの出力ルールを指定しない場合、**default** パラメータを使用して出力ルールを設定することができます。**default** パラメータを使用しない場合、モジュールはデフォルトの出力ルールを使用します。

モジュールの出力ルールを設定した後、ルールの修正あるいは削除を行う場合、*module-name* パラメータを使用する必要があります。**default** パラメータを使用して設定された新しい出力ルールはモジュールで適用されません。

複数回、モジュールのコマンドを実行した場合、最後に設定したモジュールの出力ルールが適用されます。

複数回、デフォルトモジュールのコマンドを実行した場合、最後に設定したデフォルトモジュールの出力ルールが適用されます。

例

コンソールに emergency 以上の severity の VLAN モジュールの情報を出力します。

<AP> system-view

[AP] info-center source default console deny

[AP] info-center source vlan console level emergency

以前の設定をもとにして、コンソールにシステム情報を出力しないように、VLAN モジュールの情報の出力を無効にします。

<AP> system-view

[AP] undo info-center source vlan console

3.1.11 info-center synchronous

Syntax

info-center synchronous

undo info-center synchronous

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

info-center synchronous コマンドは情報の同期出力を有効にします。

undo info-center synchronous コマンドは情報の同期出力を無効にします。

情報の同期出力とは、システムログの出力によりユーザの入力が中断された場合、中断されたところから操作を継続できるようにします。ログの出力後、編集モードのコマンドプロンプト、あるいは対話モードの“[Y/N]”の文字列を表示し、以前に入力されたコマンドおよび、コマンドプロンプトを表示させることができます。

例

情報の同期出力を有効にし、装置の現在の設定を表示する **display current-configuration** コマンドを実行します。

<AP> system-view

[AP] info-center synchronous

```
Info-center synchronous output is on
```

[AP] display current-

このとき、システムがログ情報を受信します。最初にログ情報を表示し、次に直前に入力したコマンドを表示します。この例では、display current-です。

```
%May 21 14:33:19:425 2007 AP SHELL/4/LOGIN: VTY login from 192.168.1.44
```

[AP] display current-

display current-configuration コマンドを完全に入力し、Enter キーを押下し、コマンドを実行します。

情報の同期出力を有効にし、現在の設定を保存します。（インタラクティブの情報を入力します）

<AP> system-view

[AP] info-center synchronous

```
Info-center synchronous output is on
```

[AP] save

```
The current configuration will be written to the device. Are you sure? [Y/N]:
```

このとき、システムがログ情報を受信します。最初にログ情報を表示し、次に[Y/N]を表示します。

```
%May 21 14:33:19:425 2007 AP SHELL/4/LOGIN: VTY login from 192.168.1.44
[Y/N]:
```

入力を完了するため、“Y”あるいは“N”を入力します。

3.1.12 info-center syslog min-age

Syntax

info-center syslog min-age *min-age*

undo info-center syslog min-age

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

min-age: ログの最小保存期間を指定します。設定範囲は 1～8760 時間です。

説明

info-center syslog min-age コマンドはログをログバッファに保存する最小保存期間を設定します。

undo info-center syslog min-age コマンドはデフォルトに戻します。

例

ログの最小保存期間を 168 時間に設定します。

<AP> system-view

[AP] info-center syslog min-age 168

3.1.13 info-center timestamp

Syntax

info-center timestamp { **boot** | **date** | **none** }

undo info-center timestamp

デフォルト

date

View

System view

定義済みユーザロール

network-admin

パラメータ

boot: システムが起動してからの経過時間のタイムスタンプを指定します。形式は xxx.yyy です。xxx は上位 32 ビットです。単位はミリ秒です。yyy は下位 32 ビットです。たとえば 0.21990989 は Jun 25 14:09:26:881 2007 です。

date: 現在のシステム時間のタイムスタンプを指定します。形式は MMM DD hh:mm:ss:xxx YYYY です。たとえば、Dec 8 10:12:21:708 2007 です。

- MMM: 省略した月です。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec があります。
- DD: 日です。9 日までの場合はスペースで始まります。たとえば、7 です。
- hh:mm:ss:xxx: ローカル時間です。hh の設定範囲は 00～23 で、mm と ss の設定範囲は 00～59 です。xxx の設定範囲は 0～999 です。
- YYYY: 年です。

none: 時間の情報を提供しないように指定します。

説明

info-center timestamp コマンドはコンソール、モニタ、ログバッファに送信するシステム情報のタイムスタンプの形式を設定します。

undo info-center timestamp コマンドはデフォルトに戻します。

例

ログ情報のタイムスタンプの形式を boot に設定します。

<AP> system-view

[AP] info-center timestamp boot

関連コマンド

info-center timestamp loghost

3.1.14 info-center timestamp loghost

Syntax

info-center timestamp loghost { **date** [**with-milliseconds**] | **iso** [**with-milliseconds**] | **no-year-date** | **none** }

undo info-center timestamp loghost

デフォルト

date

View

System view

定義済みユーザロール

network-admin

パラメータ

date: 現在のシステム時間のタイムスタンプを指定します。形式は mmm dd hh:mm:ss yyyy です。たとえば、Dec 8 10:12:21 2007 です。

iso: iso 8601 形式のタイムスタンプを指定します。たとえば、2009-09-21T15:32:55 です。

with-milliseconds: 日付または ISO 8601 形式でログホストに出力されるログのタイムスタンプを正確にミリ秒に設定します。ミリ秒の値は、ドットを区切り文字としてタイムスタンプ内の時刻情報に付加されます。このキーワードを指定しない場合、日付または ISO 8601 形式のタイムスタンプは、正確には秒になります。

- ミリ秒精度の日付形式のタイムスタンプの例:12 月 8 日 10:12:21.708 2018
- ISO 8601 形式でミリ秒単位の精度を持つタイムスタンプの例:2018-09-21 T 15:32:55.708

no-year-date: 年を除く現在のシステム日時のタイムスタンプを指定します。

none: 時間の情報を提供しないように指定します。

説明

info-center timestamp loghost コマンドはログホストに送信するシステム情報のタイムスタンプの形式を設定します。

undo info-center timestamp loghost コマンドはデフォルトに戻します。

例

ログホストに送信されるログのタイムスタンプ形式を **no-year-date** に設定します。

<AP> system-view

[AP] info-center timestamp loghost no-year-date

関連コマンド

info-center timestamp

3.1.15 reset logbuffer

Syntax

reset logbuffer

View

User view

定義済みユーザロール

network-admin

説明

reset logbuffer コマンドはログバッファを削除します。

例

ログバッファを削除します。

<AP> reset logbuffer

関連コマンド

display logbuffer

3.1.16 terminal debugging

Syntax

terminal debugging

undo terminal debugging

デフォルト

無効

View

User view

定義済みユーザロール

network-admin

説明

terminal debugging コマンドは現在の端末にデバッグ情報を表示することを有効にします。

undo terminal debugging コマンドは現在の端末にデバッグ情報を表示することを無効にします。

コンソールでデバッグ情報を表示する場合、以下の処理を実行します。

1) **terminal debugging** コマンドを実行します。
2) Information Center を有効にします。（デフォルトで有効です）
3) 関連するデバッグを有効にするため、**debugging** コマンドを使用します。

モニタ端末でデバッグ情報を表示する場合、以下の処理を実行します。

1) **terminal monitor** コマンド、**terminal debugging** コマンドを実行します。
2) Information Center を有効にします。（デフォルトで有効です）
3) 関連するデバッグを有効にするため、**debugging** コマンドを使用します。

このコマンドの設定は端末と装置における現在の接続のみ有効です。新しい接続が確立された場合、デフォルトに戻ります。

端末におけるデバッグ情報の表示設定はデフォルト（無効）となります。

terminal logging level 7 コマンドを実行し、現在の端末でデバッグ情報を表示することができます。**terminal debugging** コマンドとの相違を以下に示します。

- **terminal logging level 7** コマンドは現在の端末のすべてのレベル（レベル 0～レベル 7）のためにログを表示します。
- **terminal logging** コマンドは以下の severity レベルのためにログを表示します。
  - debug レベル（レベル 7）
  - **terminal logging level** のコマンドによって指定された severity 以上のレベルのために **terminal debugging** コマンドはログを表示します。

例

現在の端末でデバッグ情報を表示することを有効にします。

<AP> terminal debugging

```
The current terminal is enabled to display debugging information.
```

関連コマンド

- **terminal logging level**
- **terminal monitor**

3.1.17 terminal logging level

Syntax

terminal logging level *severity*

undo terminal logging level

デフォルト

6

View

User view

定義済みユーザロール

network-admin

パラメータ

severity: 現在の端末に出力できるログのもっとも低いレベルを指定します。設定範囲は 0～7 です。

説明

terminal logging level コマンドは現在の端末に出力できるログのもっとも低いレベルを設定します。

undo terminal logging level コマンドはデフォルトに戻します。

現在の端末に出力できるログのもっとも低いレベルを指定した場合、装置は指定されたレベル以上の severity レベルのログを出力します。たとえば、現在の端末に出力できるログのもっとも低いレベルを 6（informational）に指定した場合、0～6 の severity レベルのログを設定します。

このコマンドの設定は端末と装置における現在の接続のみ有効です。新しい接続が確立された場合、デフォルトに戻ります。

例

現在の端末に出力できるログのもっとも低いレベルを 7（debug）に設定します。

<AP> terminal logging level 7

3.1.18 terminal monitor

Syntax

terminal monitor

undo terminal monitor

デフォルト

ログの出力はコンソールで有効です。モニタ端末は無効です。

View

User view

定義済みユーザロール

network-admin

説明

terminal monitor コマンドは現在の端末にログを表示することを有効にします。

undo terminal monitor コマンドは現在の端末にログを表示することを無効にします。

このコマンドの設定は端末と装置における現在の接続のみ有効です。新しい接続が確立された場合、デフォルトに戻ります。

例

現在の端末にログを表示することを有効にします。

<AP> terminal monitor

```
The current terminal is enabled to display logs.
```

QX-W610 アクセスポイント

コマンドマニュアル

03. インタフェース

本マニュアルは以下に示す章で構成されています。

01-ループバックインタフェースと Null インタフェース

02-Ethernet インタフェース

03- Interface range

目次

このセクションのページは **3-x-x** です。

1 章 ループバックインタフェースと Null インタフェース 1-1
1.1 ループバックインタフェースと Null インタフェース設定コマンド 1-1
1.1.1 description 1-1
1.1.2 display interface loopback 1-2
1.1.3 display interface null 1-6
1.1.4 interface loopback 1-9
1.1.5 interface null 1-10
1.1.6 reset counters interface loopback 1-11
1.1.7 reset counters interface null 1-12
1.1.8 shutdown 1-13

1章 ループバックインタフェースと Null インタフェース

1.1 ループバックインタフェースとNullインタフェース設定コマンド

1.1.1 description

Syntax

description *text*

undo description

デフォルト

インタフェース名＋Interface です。（たとえば、LoopBack0 Interface です）

View

Loopback interface view

Null interface view

定義済みユーザロール

network-admin

パラメータ

text: インタフェースの説明を記載します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

description コマンドはインタフェースの説明を設定します。

undo description コマンドはデフォルトに戻します。

インタフェースの説明を設定することで、インタフェースの識別、管理しやすさを向上させることができます。

設定された説明を表示する場合、**display interface** コマンドを使用します。

例

ループバック 0 の説明を RouterID に設定します。

<AP> system-view

[AP] interface loopback 0

[AP-LoopBack1] description for RouterID

1.1.2 display interface loopback

Syntax

display interface loopback [*interface-number*] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-number: ループバックインタフェースの番号を指定します。番号は存在するループバックのインタフェースの番号です。番号を指定しない場合、装置のすべての既存のループバックインタフェースの情報を表示します。

brief: インタフェースの概要を表示します。指定しない場合、詳細なインタフェースの情報を表示します。

description: 完全なインタフェースの説明を表示します。指定しない場合、説明の最初の 27 文字のみを表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェースの情報を表示します。

説明

display interface loopback コマンドは指定した、あるいはすべての既存のループバックインタフェースの情報を表示します。

ループバックインタフェースが作成されたのち、適用されます。

loopback キーワードを指定しなかった場合、コマンドは装置のすべてのインタフェースの情報を表示します。

loopback キーワードを指定したが *interface-argument* 引数を指定しなかった場合、コマンドは存在するすべてのループバックインタフェースの情報を表示します。

例

ループバック 0 のインタフェースの詳細情報を表示します。

<AP> display interface loopback 0

```
LoopBack0
Current state: UP
Line protocol state: UP(spoofing)
```

```
Description: LoopBack0 Interface
Bandwidth: 1000 kbps
Maximum transmission unit: 1536
Internet protocol processing: Disabled
Physical: Loopback
Last clearing of counters:  Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

loopback 0 インタフェースの詳細情報を表示します（ループバックインタフェースがトラフィック統計情報の収集をサポートしていない場合）。

<AP> display interface loopback 0

```
LoopBack0
Current state: UP
Line protocol state: UP(spoofing)
Description: LoopBack0 Interface
Maximum transmit unit: 1536
Internet protocol processing : Disabled
Physical: Loopback
Last clearing of counters:  Never
```

表 1-1 コマンド出力

フィールド	説明
Current state	ループバックインタフェースの物理レイヤの状態です。 • **UP**–ループバックインタフェースがパケットの送受信を行うことができます。 • **Administratively DOWN**–インタフェースが**shutdown**コマンドにより手動でシャットダウンしています。
Line protocol state	インタフェースのリンクレイヤプロトコルの状態です。 **UP (spoofing)**はインタフェースのリンクレイヤプロトコルですが、オンデマンドのリンクあるいは準備ができていない状態です。
Description	インタフェースの説明です。
Bandwidth	インタフェースの帯域幅です。値が0の場合、このフィールドは表示されません。
Maximum transmission unit	インタフェースのMTUです。

フィールド	説明
Internet protocol processing: Disabled	インタフェースがレイヤ3パケットを処理できないことを示します。 （インタフェースにIPアドレスが設定されていない場合に表示されます）
Internet address: 1.1.1.1/32 (primary)	インタフェースのIPアドレスです。primaryはIPアドレスがプライマリIPアドレスであることを示します。
Physical: Loopback	インタフェースの物理タイプがループバックです。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最新の300秒の平均受信レートです。 ● **bytes/sec**–1秒間に受信した平均バイト数です。 ● **bits/sec**–1秒間に受信した平均ビット数です。 ● **packets/sec**–1秒間に受信した平均パケット数です。
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	最新の300秒の平均送信レートです。 ● **bytes/sec**–1秒間に送信した平均バイト数です。 ● **bits/sec**–1秒間に送信した平均ビット数です。 ● **packets/sec**–1秒間に送信した平均パケット数です。
Input: 0 packets, 0 bytes, 0 drops	インタフェースの受信パケットの総数とサイズ（単位はバイトです）と廃棄したパケット数（インタフェースがトラフィック統計情報の収集をサポートしている場合に表示されます）。
Output: 0 packets, 0 bytes, 0 drops	インタフェースの送信パケットの総数とサイズ（単位はバイトです）と廃棄したパケット数インタフェースがトラフィック統計情報の収集をサポートしている場合に表示されます）。

すべてのループバックインタフェースの概要情報を表示します。

<AP> display interface loopback brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP       Description
Loop1              UP   UP(s)     --            forLAN1
```

down 状態のすべてのループバックインタフェースの情報と原因を表示します。

<AP> display interface loopback brief down

```
Brief information on interfaces in route mode:
```

```
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
Loop1              ADM  Administratively
```

表 1-2 コマンド出力

フィールド	説明
Brief information on interfaces in route mode:	ループバックインタフェースの概要情報
Link: ADM - administratively down; Stby - standby	Linkフィールドの値を説明します。 ● **ADM**–リンクが運用上、**shutdown**コマンドでシャットダウンしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **Stby**–インタフェースがバックアップインタフェースとして動作します。プライマリインタフェースを確認するには、**display interface-backup state**コマンドを実行します。
Protocol: (s) – spoofing	Protocolフィールドの値を説明します。 (s)はスプーフィングを表します。インタフェースのリンクレイヤプロトコルがupだが、リンクがオンデマンドリンクであるかまたは存在しない場合、ProtocolフィールドはUP(s)と表示されます。本属性は通常、Null 0インタフェースおよびループバックインタフェースで表示されます。
Interface	インタフェース名
Link	インタフェースの物理リンク状態です。 ● **UP**–リンクがupです。 ● **DOWN**–リンクが物理的にdownしています。 ● **ADM**–リンクが運用上でシャットダウンしています。物理状態を回復するために、**undo shutdown**コマンドを実行します。 ● **Stby**–インタフェースがstandbyインタフェースです。
Protocol	インタフェースのデータリンクレイヤプロトコルフィールドの説明です。このフィールドは**UP(s)**と表示されます。
Primary IP	インタフェースのプライマリIPアドレスです。
Description	**description**コマンドで設定されたインタフェースの説明 display interface briefコマンドでdescriptionキーワードを指定しなかった場合、本フィールドはインタフェース説明の最初の27文字のみ表示します。display interface briefコマンドでdescriptionキーワードを指定した場合、本フィールドはインタフェース説明を完全に表示します。

フィールド	説明
Cause	インタフェースの物理リンク状態がDOWNとなった原因です。**shutdown**コマンドでインタフェースがシャットダウン状態であるとき、このフィールドは**Administratively**と表示されます。物理状態を回復するために、**undo shutdown**コマンドを実行します。

関連コマンド

- **interface loopback**
- **reset counters interface loopback**

1.1.3 display interface null

Syntax

display interface null [**0**] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

0: Null 0 インタフェースを指定します。

brief: インタフェースの概要情報を表示します。指定しない場合、詳細なインタフェースの情報を表示します。

description: 完全なインタフェースの説明を表示します。指定しない場合、説明の最初の 27 文字のみを表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェースの情報を表示します。

説明

display interface null コマンドは Null インタフェースの情報を表示します。

null キーワードを指定しなかった場合、コマンドは装置のすべてのインタフェースの情報を表示します。

null キーワードを指定したが 0 キーワードを指定しなかった場合、コマンドは Null 0 インタフェースの情報を表示します（Null インタフェースがトラフィック統計情報の収集をサポートしている場合）。

例

Null 0 インタフェースの詳細情報を表示します。（Null インタフェースがトラフィック統計情報の収集をサポートしている場合）。

<AP> display interface null 0

```
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description: NULL0 Interface
Bandwidth: 1000000 kbps
Maximum transmission unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV
Last clearing of counters: Never
Last 300 seconds input rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate:  0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

Null 0 インタフェースの概要情報を表示します。（Null インタフェースがトラフィック統計情報の収集をサポートしていない場合）。

<AP> display interface null 0

```
NULL0
Current state: UP
Line protocol state: UP(spoofing)
Description:  NULL0 Interface
Maximum transmit unit: 1500
Internet protocol processing: Disabled
Physical: NULL DEV
Last clearing of counters: Never
```

Null 0 インタフェースの概要情報を表示します。

<AP> display interface null 0 brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface          Link Protocol Primary IP       Description
NULL0              UP   UP(s)    --
```

コマンド出力は表 1-1、表 1-2 を参照してください。

関連コマンド

- **interface null**
- **reset counters interface null**

1.1.4 interface loopback

Syntax

interface loopback *interface-number*

undo interface loopback *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

*interface-numbe*r: ループバックインタフェースを指定します。値は 0 です。

説明

interface loopback コマンドはループバックインタフェースを作成し、loopback interface view に移行します。

undo interface loopback コマンドはループバックインタフェースを削除します。

ループバックインタフェースの物理レイヤの状態とリンクレイヤプロトコルは手動でシャットダウンしない限り、常に up 状態です。このため、以下の目的に使用することができます。

- インタフェースの物理状態に影響されることなく、接続状態となります。
- 接続の信頼性を改善します。

たとえば、次のようなことができます。

- FTP 接続を確立するために送信元インタフェースとしてループバックインタフェースを設定
- BGP においてルータ ID としてのループバックインタフェースアドレス。

例

インタフェースループバック 0 を作成します。

<AP> system-view

[AP] interface loopback 0

[AP-LoopBack0]

1.1.5 interface null

Syntax

interface null 0

デフォルト

装置は 1 つの Null インタフェース(Null 0)があります。作成あるいは削除することができません。

View

System view

定義済みユーザロール

network-admin

パラメータ

0: Null 0 インタフェースを指定します。Null インタフェースの番号は常に 0 です。

説明

interface null コマンドは null interface view に移行します。

例

null 0 interface view に移行します。

<AP> system-view

[AP] interface null 0

[AP-NULL0]

1.1.6 reset counters interface loopback

Syntax

reset counters interface loopback [*interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface-number: ループバックインタフェースの番号を指定します。番号は存在するループバックのインタフェースの番号です。番号を指定しない場合、装置のすべての既存するループバックインタフェースの統計情報を削除します。

説明

reset counters interface loopback コマンドは指定した、あるいはすべての既存のループバックインタフェースの統計情報を削除します。

一定期間、ループバックインタフェースのトラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除するために **reset counters interface** [**loopback** [*interface-number*]]コマンドを使用します。その後、自動で統計情報を収集します。

このコマンドは少なくとも 1 つのループバックインタフェースが作成されている場合のみ有効です。

例

ループバックインタフェース 0 の統計情報を削除します。

<AP> reset counters interface loopback 0

関連コマンド

display interface loopback

1.1.7 reset counters interface null

Syntax

reset counters interface null [**0**]

View

User view

定義済みユーザロール

network-admin

パラメータ

0: Null 0 インタフェースを指定します。Null インタフェースの番号は常に 0 です。

説明

reset counters interface null コマンドは Null インタフェースの統計情報を削除します。

一定期間、Null インタフェースのトラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除するために**reset counters interface** [**null** [**0**]]コマンドを使用します。その後、自動で統計情報を収集します。

例

Null 0 インタフェースの統計情報を削除します。

<AP> reset counters interface null 0

関連コマンド

display interface null

1.1.8 shutdown

Syntax

shutdown

undo shutdown

デフォルト

up

View

Loopback interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはループバックインタフェースをシャットダウンします。

undo shutdown コマンドはループバックインタフェースを up にします。

このコマンドはインタフェースの接続を切断し、通信を行うためのインタフェースを無効にするため、**shutdown** コマンドを使用する際には影響を考慮してください。

例

ループバックインタフェース Loopback 0 をシャットダウンします。

<AP> system-view

[AP] interface loopback 0

[AP-LoopBack0] shutdown

目次

このセクションのページは **3-x-x** です。

2 章 Ethernet インタフェース 2-1
2.1 共通 Ethernet インタフェース設定コマンド 2-1
2.1.1 broadcast-suppression 2-1
2.1.2 description 2-2
2.1.3 display counters 2-3
2.1.4 display counters rate 2-5
2.1.5 display interface 2-6
2.1.6 duplex 2-18
2.1.7 flow-interval 2-19
2.1.8 interface 2-20
2.1.9 jumboframe enable 2-21
2.1.10 multicast-suppression 2-22
2.1.11 reset counters interface 2-23
2.1.12 shutdown 2-24
2.1.13 speed 2-24

2章 Ethernet インタフェース

2.1 共通Ethernetインタフェース設定コマンド

2.1.1 broadcast-suppression

Syntax

broadcast-suppression { *ratio* **| pps** *max-pps* **| kbps** *max-kbps* **}**

undo broadcast-suppression

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio:ブロードキャスト抑制しきい値をインタフェース帯域幅のパーセンテージで設定します。この引数の値の範囲は 0 から 100 です。値が小さいほど、通過できるブロードキャストトラフィックが少なくなります。

pps *max-pps*: インタフェースが 1 秒あたりに転送できるブロードキャストパケットの最大数を指定します。*max-pps* 引数の値の範囲は、インタフェース帯域幅の 0~1.4881 倍(pps 単位)です。

kbps *max-kbps*: イーサネットインタフェースが 1 秒あたりに転送できるブロードキャストトラフィックの最大キロビット数を指定します。この引数の値の範囲は、0~インタフェース帯域幅(kbps 単位)です。

説明

broadcast-suppression コマンドはブロードキャスト抑制しきい値を設定し、ブロードキャスト抑制を有効にします。

undo broadcast-suppression コマンドはブロードキャスト抑制を無効にします。

ブロードキャストストーム抑制機能は、ブロードキャストトラフィックのサイズをインタフェースのしきい値に制限します。インタフェース上のブロードキャストトラフィックがこのしきい値を超えると、トラフィックがこのしきい値を下回るまで、システムはパケットを破棄します。

例

GigabitEthernet 1/0/1 でブロードキャスト抑制しきい値を 10000kbps に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] broadcast-suppression kbps 10000

2.1.2 description

Syntax

description *text*

undo description

デフォルト

インタフェース名＋Interface です。（たとえば GigabitEthernet1/0/1 Interface です）

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

text: インタフェースの説明を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。

説明

description コマンドはインタフェースの説明を変更します。

undo description コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の説明を lan-interface に変更します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] description lan-interface

2.1.3 display counters

Syntax

display counters { **inbound** | **outbound** } **interface** [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: 受信トラフィックの統計情報を表示します。

outbound: 送信トラフィックの統計情報を表示します。

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

説明

display counters コマンドはインタフェースのトラフィックの統計情報を表示します。

このコマンドは **flow-interval** コマンドで指定されたポートの統計情報を収集する間隔内のトラフィックの統計情報を表示します。

Ethernet インタフェースのトラフィックの統計情報を削除する場合、**reset counters interface** コマンドを使用します。

インタフェースタイプを指定しない場合、すべてのインタフェースのトラフィックの統計情報を表示します。

インタフェースタイプを指定し、番号を指定しない場合、指定したインタフェースタイプのすべてのインタフェースのトラフィックの統計情報を表示します。

インタフェースタイプと番号を指定した場合、指定したインタフェースのすべてのトラフィックの統計情報を表示します。

例

すべての GigabitEthernet インタフェースの受信トラフィックの統計情報を表示します。

<AP> display counters inbound interface GigabitEthenet

```
Interface        Total (pkts)    Broadcast (pkts)    Multicast (pkts)  Err (pkts)
GE1/0/1                 100                 100                   0           0

 Overflow: More than 14 digits (7 digits for column "Err").
      --: Not supported.
```

表 2-1 コマンド出力

フィールド	説明
Interface	インタフェース名の省略名です。
Total (pkts)	インタフェースを通して送受信したパケットの総数です。
Broadcast (pkts)	インタフェースを通して送受信したブロードキャストパケットの総数です。RPR物理ポートでは、送受信されたすべてのブロードキャスト、マルチキャストパケットはマルチキャストパケットとして表示されます。
Multicast (pkts)	インタフェースを通して送受信したマルチキャストパケットの総数です。RPR物理ポートでは、送受信されたすべてのブロードキャスト、マルチキャストパケットはマルチキャストパケットとして表示されます。
Err (pkts)	インタフェースを通して送受信したエラーパケットの総数です。
Overflow: More than 14 digits (7 digits for column "Err")	以下のときに**Overflow**と表示します。 ● エラーフィールド値のデータ長が10進数で7桁を超えました。 ● 非エラーフィールド値のデータ長が10進数で14桁を超えました。
--: Not supported	統計情報をサポートしていません。

関連コマンド

- **flow-interval**
- **reset counters interface**

2.1.4 display counters rate

Syntax

display counters rate { **inbound** | **outbound** } **interface** [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

inbound: 受信トラフィックレートの統計情報を表示します。

outbound: 送信トラフィックレートの統計情報を表示します。

interface-type: インタフェースのタイプを指定します。

interface-number: インタフェースの番号を指定します。

説明

display counters rate コマンドは最後のサンプリング間隔からの up 状態のインタフェースのトラフィックレートの統計情報を表示します。

統計情報は up 状態のインタフェースのみ適用されます。

インタフェースタイプを指定しない場合、すべてのインタフェースのトラフィックレートの統計情報を表示します。

インタフェースタイプを指定し、インタフェースの番号を指定しない場合、指定されたタイプのすべての up 状態のインタフェースのトラフィックレートの統計情報を表示します。

インタフェースタイプ、インタフェースの番号を指定した場合、指定したインタフェースのトラフィックレートの統計情報を表示します。

down 状態のインタフェースが指定されている場合、システムはコマンドをサポートしていないと表示されます。

例

すべての GigabitEthernet の受信トラフィックレートの統計情報を表示します。

<AP> display counters rate inbound interface gigabitethernet

```
Usage: Bandwidth utilization in percentage
Interface          Usage (%)   Total (pps)   Broadcast (pps)   Multicast (pps)
GE1/0/1                    3           200               100               100
GE1/0/2                    5           300               200               100
```

```
GE1/0/3                 5            300             200                 100

 Overflow: More than 14 digits.
      --: Not supported.
```

表 2-2 コマンド出力

フィールド	説明
Interface	インタフェース名の省略名です。
Usage (%)	最後のサンプリング間隔中にインタフェースで送受信したパケットの平均レートです。単位は%です。
Total (pkts/sec)	最後のサンプリング間隔中に送受信したユニキャストパケットの平均レートです。単位はppsです。
Broadcast (pkts/sec)	最後のサンプリング間隔中に送受信したブロードキャストパケットの平均レートです。単位はppsです。RPR物理ポートでは、送受信されたすべてのブロードキャスト、マルチキャストパケットはマルチキャストパケットとして表示されます。
Multicast (pkts/sec)	最後のサンプリング間隔中に送受信したマルチキャストパケットの平均レートです。単位はppsです。RPR物理ポートでは、送受信されたすべてのブロードキャスト、マルチキャストパケットはマルチキャストパケットとして表示されます。
Overflow: more than 14 decimal digits	データ長が10進数で14桁を超えたときに、**Overflow**と表示します。
--: not supported	統計情報をサポートしていません。

関連コマンド

- **flow-interval**
- **reset counters interface**

2.1.5 display interface

Syntax

display interface [*interface-type* [*interface-number*]] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

brief: 概要情報を表示します。指定しない場合、コマンドは詳細なインタフェース情報を表示します。

description: インタフェースの説明をすべて表示します。指定しない場合、インタフェースの説明の最初の 27 文字のみ表示します。

down: down 状態のインタフェースの情報と原因を表示します。指定しない場合、すべての状態のインタフェース情報を表示します。

説明

display interface コマンドは Ethernet インタフェースの情報を表示します。

インタフェースタイプを指定しない場合、すべてのインタフェースの情報を表示します。

インタフェースタイプを指定し、番号を指定しない場合、指定したタイプのすべてのインタフェースの情報を表示します。

インタフェースタイプと番号を指定した場合、指定したインタフェースの情報を表示します。

例

レイヤ 2 インタフェースの GigabitEthernet 1/0/1 の詳細情報を表示します。

<AP> display interface gigabitethernet 1/0/1

```
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 000c-2963-b767
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 100000kbps
Loopback is not set
Media type is twisted pair,port hardware type is 1000_BASE_T_AN_SFP
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frame to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
```

```
Unicast max-ratio: 100%
PVID: 1
Port link-type: Access
Tagged VLANs:   None
UnTagged VLANs: 1
Port priority: 2
Last link flapping: 6 hours 39 minutes 25 seconds
Last clearing of counters:  14:34:09 Tue 11/01/2017
Current system time: 2017-07-18 17:05:40 UTC+00:08:00
Last time when physical state changed to up: -
Last time when physical state changed to down: 2017-07-18 16:05:40 UTC+00:08:00
Peak input rate: 0 bytes/sec, at 2017-07-17 22:06:19
Peak output rate: 0 bytes/sec, at 2017-07-17 22:06:19
Last 300 second input:  0 packets/sec 0 bytes/sec -%
Last 300 second output:  0 packets/sec 0 bytes/sec -%
Input (total):  0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input (normal):  0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Input:  0 input errors, 0 runts, 0 giants, 0 throttles
        0 CRC, 0 frame, 0 overruns, 0 aborts
        0 ignored, 0 parity errors
Output (total): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output (normal): 0 packets, 0 bytes
        0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
Output: 0 output errors, 0 underruns, 0 buffer failures
        0 aborts, 0 deferred, 0 collisions, 0 late collisions
        0 lost carrier, 0 no carrier
```

表 2-3 コマンド出力

フィールド	説明
Current state	Ethernetインタフェースの状態です。 ● **Administratively DOWN—shutdown**コマンドでインタフェースがシャットダウンしています。インタフェースは運用上においてdownしています。 ● **DOWN—shutdown**コマンドでシャットダウンしていませんが、物理的にdownしています。（Ethernetケーブルが物理的に接続されていない、あるいはリンクに失敗している可能性があります） ● **DOWN (Link-Aggregation interface down)— shutdown**コマンドでアグリゲートインタフェースがシャットダウンし

フィールド	説明
	ています。 • **DOWN (Tunnel-Bundle administratively down)— shutdown**コマンドでインタフェースが所属するトンネルバンドルインタフェースがダウンしています。装置は現在のソフトウェアバージョンでは、本フィールドをサポートしません。 • **ETH-rddc Shutdown**—インタフェースはRethモジュールによりダウンしています。装置は現在のソフトウェアバージョンでは、本フィールドをサポートしません。 • **mac-address moving down**—MACアドレスの移動の抑制機能によりインタフェースがシャットダウンしています。 • **Storm-Constrain**—ストーム抑止機能が不明なユニキャストトラフィック、マルチキャストトラフィック、ブロードキャストトラフィックの上限に到達したことを検出したため、インタフェースがシャットダウンしています。 • **STP DOWN**—BPDUガード機能によりインタフェースがシャットダウンしています。 • **UP**—インタフェースが運用上も物理的にも起動している状態です。

Line protocol state	インタフェースのリンクレイヤの状態です。リンクレイヤのパラメータのネゴシエーションによって決まります。
	• **UP**—インタフェースがリンクレイヤでupしています。
	• **UP (spoofing)**—インタフェースがリンクレイヤでupしていますが、オンデマンドのリンクあるいは準備ができていない状態です。この属性はNullインタフェースとループバックインタフェースの一般的な状態です。
	• **DOWN**—インタフェースがリンクレイヤでdownしています。
	• **DOWN (*protocols*)**—インタフェースが括弧内のプロトコルにより、リンクレイヤでdownしています。
	  • **DLDP**—リンクが片方向であるとDLDPが検出したため、インタフェースがリンクレイヤでdownしています。
	  • **LAGG**—アグリゲートインタフェースがSelectedポートでないため、インタフェースがリンクレイヤでdownしています。
	  • **BFD**—リンク障害を検出したためインタフェースがリンクレイヤでdownしています。

フィールド	説明
	• *protocol*にMACSECを含む場合、MACSECが暗号化パラメータのネゴシエーションに失敗したため、インタフェースがリンクレイヤでdownしています。装置は現在のソフトウェアバージョンでは本フィールドをサポートしていません。
Bandwidth	インタフェースの予期された帯域幅です。
Maximum transmission unit	インタフェースのMTUです。
Internet protocol processing: Disabled	インタフェースにIPアドレスが設定されておらず、IPパケットを処理できません。
Internet address	インタフェースのIPアドレスを表示します。**primary**はIPアドレスがプライマリIPアドレスであることを示します。
IP packet frame type	IPv4パケットのフレームタイプです。
hardware address	インタフェースのMACアドレスです。
IPv6 packet frame type	IPv6パケットのフレームタイプです。
Port priority	インタフェースのプライオリティです。
Loopback is set internal	インタフェースで内部ループバックテストが動作しています。このフィールドは内部ループバックテストの設定が行われた場合に表示されます。
Loopback is set external	インタフェースで外部ループバックテストが動作しています。このフィールドは外部ループバックテストの設定が行われた場合に表示されます。
Loopback is not set	インタフェースでループバックテストが動作していません。このフィールドはループバックテストの設定が行われていない場合に表示されます。
10Mbps-speed mode	インタフェースが10Mbpsで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
100Mbps-speed mode	インタフェースが100Mbpsで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
1000Mbps-speed mode	インタフェースが1000Mbpsで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
Unknown-speed mode	通信速度のネゴシエーションに失敗あるいはインタフェースが物理的に切断しているため、インタフェースの速度が不明です。

フィールド	説明
half-duplex mode	インタフェースがhalfの動作モードで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
full-duplex mode	インタフェースがfullの動作モードで動作しています。このフィールドは通信速度の設定とリンクパラメータのネゴシエーションの結果によって異なります。
unknown-duplex mode	通信モードのネゴシエーションに失敗あるいはインタフェースが物理的に切断しているため、インタフェースの通信モードが不明です。
Link speed type is autonegotiation	**speed auto**コマンドでインタフェースに設定されています。
Link speed type is force link	**speed**コマンドで通信速度がインタフェースに設定されています。たとえば100Mbpsです。
link duplex type is autonegotiation	**duplex auto**コマンドでインタフェースに設定されています。
link duplex type is force link	**duplex**コマンドで通信モードがインタフェースに設定されています。たとえばhalfあるいはfullです。
Flow-control is not enabled	インタフェースでフローコントロールが無効です。このフィールドは設定とリンクパラメータのネゴシエーションの結果によって異なります。
Maximum frame length	インタフェースの最大フレーム長です。
Allow jumbo frame to pass	インタフェースがジャンボフレームをサポートしています。
Broadcast max-	ブロードキャストストーム抑制のしきい値です。単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
Multicast max-	マルチキャストストーム抑制のしきい値です。単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
Unicast max-	ユニキャストストーム抑制のしきい値です。単位はratio、pps、kbpsです。しきい値のユニットは設定に依存します。
PVID	インタフェースのポートVLANのID（PVID）です。
Port link-type	インタフェースのリンクタイプです。 ● accessです。 ● trunkです。 ● hybridです。
Tagged VLANs	VLANタグを削除しないでパケット送信するVLANです。
Untagged VLANs	VLANタグを削除したのち、パケット送信するVLANです。

フィールド	説明
VLAN Passing	パケットがポートで転送することができるVLANです。VLANはすでに作成されている必要があります。
VLAN permitted	パケットがポートで許可されたVLANです。
Trunk port encapsulation	トランクポートのカプセル化のプロトコルタイプです。
Last link flapping	リンクがフラッピングしてからの経過時間です。 **Never**は装置が起動してから一度もリンクのフラッピングが発生していないことを示します。
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 second input: 0 packets/sec 0 bytes/sec 0% Last 300 second output: 0 packets/sec 0 bytes/sec 0%	過去300秒以内の平均送受信トラフィックです。単位はpps、bpsです。最大インタフェース速度に対する実際の速度の比率です。ハイフン（-）はサポートしてないことを示します。
Input(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの受信トラフィックの統計情報（パケット、バイト数）です。すべての正常な受信パケット、異常なパケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドを示します。 ● ユニキャストパケットの受信数です。 ● ブロードキャストの受信数です。 ● マルチキャストの受信数です。 ● pauseフレームの受信数です。 ハイフン（-）はサポートしてないことを示します。
Input(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの正常な受信トラフィックとの統計情報（パケット、バイト数）です。すべての正常な受信パケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドを示します。 ● 正常なユニキャストパケットの受信数です。 ● 正常なブロードキャストの受信数です。 ● 正常なマルチキャストの受信数です。 ● 正常なpauseフレームの受信数です。 ハイフン（-）はサポートしてないことを示します。
input errors	受信エラーパケットの統計情報です。
runts	以下の状況にある受信フレーム数です。 ● 64バイト長未満のフレームです。

フィールド	説明
	● 不正なフォーマットのフレームです。 ● 有効なCRCが含まれるフレームです。
giants	インタフェースでサポートされるフレーム長よりも長い受信フレーム数です。 ジャンボフレームをサポートしていないインタフェースでは、最大フレーム長は以下です。 ● 1518バイト（VLANタグなし）。 ● 1522バイト（VLANタグつき）。 ジャンボフレームをサポートしているインタフェースでは、giantsはインタフェースを通過することを許可されたフレームの最大長より長いフレームを示します。
throttles	整数倍バイト長でない入力フレームの数です。
CRC	正常なフレーム長ですが、CRCエラーが含まれている受信フレームの総数です。
frame	CRCエラーが含まれ、整数バイトでない受信フレームの総数です。
overruns	ポートの受信レートがキューの容量を超過したため、廃棄されたパケット数です。
aborts	不正な受信パケットの総数です。 ● **Fragment frames**—64バイトよりも短いフレームのCRCエラーフレームです。フレーム長は整数あるいは非整数の値です。 ● **Jabber frames**—インタフェースでサポートされている最大フレーム長よりも長いフレームのCRCエラーフレームです。フレーム長は整数あるいは非整数の値です。 　● ジャンボフレームを許可しない場合、最大フレーム長は1518バイト（VLANタグなし）あるいは1540バイト（VLANタグつき）よりも長いCRCエラーフレームを示します。 　● ジャンボフレームを許可する場合、jabberフレームはインタフェースを通過することを許可されたフレームの最大長より長いフレームを示します。 ● **Symbol error frames**—少なくとも1つ以上の定義されていないシンボルを含むフレームです。 ● **Unknown operation code frames**—MAC制御フレームでpauseフレームでないフレームです。 ● **Length error frames**—802.3のレングスフィールドが実際のフレーム長に合致していないフレームです。（46～1500バイトです）

フィールド	説明
ignored	ポートの受信バッファの能力不足により、インタフェースに廃棄された受信フレームの数です。
parity errors	パリティエラーのフレームの総数です。
Output(total): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの送信トラフィックの統計情報（パケット、バイト数）です。すべての正常な送信パケット、異常なパケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドを示します。 ● ユニキャストパケットの送信数です。 ● ブロードキャストの送信数です。 ● マルチキャストの送信数です。 ● pauseフレームの送信数です。 ハイフン（-）はサポートしてないことを示します。
Output(normal): 0 packets, 0 bytes 0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses	フィールドの1行目はインタフェースの正常な送信トラフィックとの統計情報（パケット、バイト数）です。すべての正常な送信パケット、正常なpauseフレームがカウントされます。 2行目の4つのフィールドを示します。 ● 正常なユニキャストパケットの送信数です。 ● 正常なブロードキャストの送信数です。 ● 正常なマルチキャストの送信数です。 ● 正常なpauseフレームの送信数です。 ハイフン（-）はサポートしてないことを示します。
output errors	送信エラーパケットの統計情報です。
underruns	ポートの送信レートがキューの容量を超過したため、廃棄されたパケット数です。これは低確率でハードウェアの異常を示します。
buffer failures	ポートの送信バッファの能力不足により、インタフェースに廃棄されたパケットの数です。
aborts	Ethernetコリジョンなどにより、転送に失敗したパケット数です。
deferred	検出したコリジョンにより、フレームを遅延させた数です。
collisions	フレームの送信中にEthernetコリジョンが検出されたため、転送を停止したフレーム数です。
late collisions	最初の512ビットをネットワークに送信した後にコリジョンが検出され、フレームの送信が遅延した回数です。
lost carrier	送信中にキャリアが失われた回数です。このカウンタは、キャリアが失われたときに増加し、シリアルWANインタフェ

フィールド	説明
	ースに適用されます。
no carrier	フレームを送信しようとしたときポートがキャリアの検出に失敗した回数です。このカウンタは、ポートがキャリアの検出に失敗したときに増加し、シリアルWANインタフェースに適用されます。
Peak input rate	受信トラフィックレートのピークレートと受信トラフィックのピークが発生したときの時間です。ピークレートの単位はbpsです。
Peak output rate	送信トラフィックレートのピークレートと送信トラフィックのピークが発生したときの時間です。ピークレートの単位はbpsです。

すべてのインタフェースの概要情報を表示します。

<AP> display interface brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing

Interface           Link Protocol Primary IP     Description
InLoop0             UP   UP(s)    --
NULL0               UP   UP(s)    --
Vlan1               UP   UP      192.168.100.150

Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface           Link Speed   Duplex Type PVID Description
GE1/0/1             DOWN auto    A      A    1
WLAN-Radio1/0/1      UP   --      --     --   --
WLAN-Radio1/0/2      UP   --      --     --   --
```

インタフェースの完全な説明を含む GigabitEthernet 1/0/1 の概要情報を表示します。

<AP> display interface gigabitethernet 1/0/1 brief description

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
```

```
Interface          Link Speed   Duplex Type PVID Description
GE1/0/1            UP   100M(a) F(a)   A    1    aaaaaaaaaaaa
```

down 状態のインタフェースの情報と原因を表示します。

<AP> display interface brief down

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Interface          Link Cause
GE1/0/1            DOWN Not connected
```

表 2-4 コマンド出力

フィールド	説明
Brief information on interfaces in route mode:	レイヤ3インタフェースの概要情報です。
Interface	インタフェース名です。
Link	インタフェースの物理リンク状態です。 ● **UP**—リンクがupです。 ● **DOWN**—リンクが物理的にdownしています。 ● **ADM**—リンクが運用上、**shutdown**コマンドでシャットダウンしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **Stby**—インタフェースがバックアップインタフェースとして動作します。
Protocol	インタフェースのリンクレイヤの状態です。 ● **UP**－インタフェースのリンクがupです。 ● **DOWN**－インタフェースのリンクがdownです。 ● **UP(s)**—インタフェースのリンクがオンデマンドリンクあるいは準備ができていない状態です。ここで（**s**）はスプーフィングのフラグを示します。Nullインタフェース、ループバックインタフェースで表示されます。
Primary IP	インタフェースのプライマリIPアドレスです。ハイフン（**--**）はIPアドレスが設定されていないことを示します。
Description	インタフェースの説明です。
Brief information of interfaces in bridge mode:	レイヤ2インタフェースの概要情報です。
Type: A - access; T - trunk; H – hybrid	インタフェースのリンクタイプのオプションです。
Speed	インタフェースの通信速度です。 インタフェースが自動でネゴシエーションされる場合、（**a**）で示されたオートネゴシエーションのフラグが含まれま

フィールド	説明
	す。インタフェースにオートネゴシエーションが設定されているがオートネゴシエーションが開始していない場合、**auto**と表示されます。
Duplex	インタフェースの通信モードです。 ● **A**—オートネゴシエーションです。インタフェースのオートネゴシエーションの通信モードがautoに設定されているがオートネゴシエーションが開始していません。 ● **F**—通信モードがfullです。 ● **F(a)**— 通信モードがfullでオートネゴシエートされています。 ● **H**—通信モードがhalfです。 ● **H(a)**—通信モードがhalfでオートネゴシエートされています。
Type	インタフェースのリンクタイプです。 ● **A**—アクセスです。 ● **H**—ハイブリッドです。 ● **T**—トランクです。
PVID	ポートVLANのIDです。
Cause	インタフェースの物理リンク状態がDOWNとなった原因です。 ● **Administratively**—**shutdown**コマンドでインタフェースがシャットダウンしています。インタフェースは運用上においてdownしています。物理状態を回復する場合、**undo shutdown**コマンドを実行します。 ● **DOWN (Link-Aggregation interface down)**—アグリゲートインタフェースがシャットダウンしているとき、アグリゲートインタフェースのすべてのメンバポートの物理状態がdownです。 ● **DOWN (Loopback detection down)**—ループバック検出モジュールがループバックを検出したため、ポートがシャットダウンしています。 ● **DOWN (Monitor-Link uplink down)**—モニタリンクモジュールがアップリンクのダウンを検出したため、ポートがシャットダウンしています。 ● **Not connected**—物理接続がありません。（ネットワークが切断された、あるいは故障している可能性があります） ● **Storm-Constrain**—不明なユニキャストトラフィック、マルチキャストトラフィック、ブロードキャストトラフィックが上限を超過したため、ポートがシャットダウンして

フィールド	説明
	います。 • **STP DOWN**—STP BPDUガード機能によってポートがシャットダウンしています。 • **Standby**—インタフェースがstandby状態です。

関連コマンド

reset counters interface

2.1.6 duplex

Syntax

duplex { **auto** | **full** | **half** }

undo duplex

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

auto: ピアとの動作モードをオートネゴシエーションに設定します。

full: インタフェースが同時にパケットの送受信を行えるように通信モードを full（全 2 重モード）に設定します。

half: インタフェースが受信時にパケットの送信あるいは受信のみを行えるように動作モードを half（半 2 重モード）に設定します。1000Mbps で動作する RJ-45 ポートは、未サポートです。

説明

duplex コマンドはインタフェースの通信モードを設定します。

undo duplex コマンドはインタフェースの通信モードをデフォルトに戻します。

例

GigabitEthernet 1/0/1 の通信モードを full に設定します。

<AP> system-view

[System] interface gigabitethernet 1/0/1

[System-GigabitEthernet1/0/1] duplex full

2.1.7 flow-interval

Syntax

flow-interval *interval*

undo flow-interval

デフォルト

300 秒

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval: ポートの統計情報を収集する間隔を設定します。設定範囲は 5～300 で、5 の倍数にする必要があります。

説明

flow-interval コマンドはポートの統計情報を収集する間隔を設定します。

undo flow-interval コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の統計情報を収集する間隔を 100 秒に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] flow-interval 100

2.1.8 interface

Syntax

interface *interface-type interface-number*

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

説明

interface コマンドは interface view に移行します。

例

GigabitEthernet 1/0/1 の interface view に移行します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[System-GigabitEthernet1/0/1]

2.1.9 jumboframe enable

Syntax

jumboframe enable

undo jumboframe enable

デフォルト

1600 バイトまでのジャンボフレームを許可します。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

jumboframe enable コマンドは指定したフレーム長以内のジャンボフレームの通過を許可します。

undo jumboframe enable コマンドはジャンボフレームの通過を拒否します。

例

GigabitEthernet 1/0/1 でジャンボフレームの通過を許可します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] jumboframe enable

2.1.10 multicast-suppression

メモ：

multicast-suppression コマンドはソフトウェアバージョン 7.2.56 を含む以降のソフトウェアからサポートしています。

Syntax

multicast-suppression { *ratio* **| pps** *max-pps* **| kbps** *max-kbps* **}**

undo multicast-suppression

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

ratio:マルチキャスト抑制しきい値をインタフェース帯域幅のパーセンテージで設定します。この引数の値の範囲は 0 から 100 です。値が小さいほど、通過できるマルチキャストトラフィックが少なくなります。

pps *max-pps*: インタフェースが 1 秒あたりに転送できるマルチキャストパケットの最大数を指定します。*max-pps* 引数の値の範囲は、インタフェース帯域幅の 0~1.4881 倍(pps 単位)です。

kbps *max-kbps*: イーサネットインタフェースが 1 秒あたりに転送できるマルチキャストトラフィックの最大キロビット数を指定します。この引数の値の範囲は、0~インタフェース帯域幅(kbps 単位)です。

説明

multicast-suppression コマンドはマルチキャスト抑制しきい値を設定し、マルチキャスト抑制を有効にします。

undo multicast-suppression コマンドはマルチキャスト抑制を無効にします。

マルチキャストストーム抑制機能は、マルチキャストトラフィックのサイズをインタフェースのしきい値に制限します。インタフェース上のマルチキャストトラフィックがこのしきい値を超えると、トラフィックがこのしきい値を下回るまで、システムはパケットを破棄します。

例

GigabitEthernet 1/0/1 でマルチキャスト抑制しきい値を 10000kbps に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] multicast-suppression kbps 10000

2.1.11 reset counters interface

Syntax

reset counters interface [*interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface-type: インタフェースタイプを指定します。

interface-number: インタフェース番号を指定します。

説明

reset counters interface コマンドはインタフェースの統計情報を削除します。

一定期間、トラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除し、このコマンドを使用します。

インタフェースタイプを指定しない場合、すべてのインタフェースの統計情報を削除します。

インタフェースタイプのみを使用する場合、インタフェースタイプのすべてのインタフェースの統計情報を削除します。

インタフェースタイプとインタフェース番号を指定した場合、指定したインタフェースの統計情報を削除します。

例

GigabitEthernet 1/0/1 の統計情報を削除します。

<AP> reset counters interface gigabitethernet 1/0/1

関連コマンド

- **display counters interface**
- **display counters rate interface**

- **display interface**

2.1.12 shutdown

Syntax

shutdown

undo shutdown

デフォルト

インタフェースはアップ状態です。

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドはインタフェースをシャットダウンします。

undo shutdown コマンドはインタフェースをアップ状態にします。

あるインタフェースの設定が適用されていることを確認するため、インタフェースをシャットダウンし、その後アップ状態にする必要があることがあります。

shutdown コマンドと **loopback** コマンドを同時に設定することはできません。

例

GigabitEthernet 1/0/1 をシャットダウンし、その後アップ状態にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] shutdown

[AP-GigabitEthernet1/0/1] undo shutdown

2.1.13 speed

Syntax

speed { **10** | **100** | **1000** | **auto** }

undo speed

デフォルト

auto

View

Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

10: インタフェースの通信速度を 10Mbps に設定します。

100: インタフェースの通信速度を 100Mbps に設定します。

1000: インタフェースの通信速度を 1000Mbps に設定します。

auto: ピアとの通信速度をオートネゴシエーションに設定します。

説明

speed コマンドはインタフェースの通信速度を設定します。

undo speed コマンドはデフォルトに戻します。

キーワードに対するインタフェースのサポートは、インタフェースの種類によって異なります。ピアのインタフェースの通信速度に一致するように **speed** コマンドを使用します。

例

GigabitEthernet 1/0/1 の通信速度を auto に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] speed auto

目次

このセクションのページは **3-x-x** です。

3 章 Interface range 3-1
3.1 Interface range 設定コマンド 3-1
3.1.1 display interface range 3-1
3.1.2 interface range 3-2
3.1.3 interface range name 3-4

3章 Interface range

3.1 Interface range設定コマンド

3.1.1 display interface range

Syntax

display interface range [**name** *name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *name*: インタフェースレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。指定しない場合、**interface range name** コマンドで作成されたすべてのインタフェースレンジの情報を表示します。

説明

display interface range コマンドは **interface range name** コマンドを使用して作成されたインタフェースレンジの情報を表示します。

例

interface range name コマンドを使用して作成されたすべての既存のインタフェースレンジの情報を表示します。

<AP> display interface range

```
Interface range name test GigabitEthernet1/0/1
```

出力は以下のことを示します。

- インタフェースレンジ **test** に GigabitEthernet 1/0/1 が追加されました。

関連コマンド

interface range name

3.1.2 interface range

Syntax

interface range *interface-list*

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-list: インタフェースを指定します。半角スペースで区切り、インタフェースを指定します。インタフェースの範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。*interface-type interface-number1* **to** *interface-type interface-number2* を指定したとき、*interface-number2* は *interface-number1* 以上の値にしてください。

説明

interface range コマンドはインタフェースレンジを作成し、interface range view に移行します。

同じ機能を 1 つずつインタフェースに設定する代わりに、interface range view に移行して、複数のインタフェースをまとめて実行することができます。たとえば、インタフェースの範囲をシャットダウンするため、interface range view で **shutdown** コマンドを実行します。

interface range コマンドで作成されたインタフェースレンジはカレントコンフィグレーションに保存されません。インタフェースレンジは繰り返し使用することができません。使用したインタフェースレンジを繰り返し使用する場合、**interface range name** コマンドを使用します。

interface range view では、最初に指定したインタフェースでサポートされるコマンドのみが有効です。最初に指定するインタフェースは **interface range** コマンドで指定されます。インタフェースレンジのコマンドを表示する場合、interface range view に移行し、インタフェースのコマンドラインでクエスチョン（**?**）を入力します。

interface range view でコマンドを実行した後、以下のいずれかの状態が起こる可能性があります。

- システムは、エラーメッセージを表示し interface range view にとどまります。それは、メンバインタフェースで実行が失敗したことを意味します。
  - □ 最初のメンバインタフェースで失敗した場合、コマンドはどのメンバインタフェースでも実行されません。
  - □ 最初のメンバインタフェース以外で失敗した場合、コマンドは他のメンバインタフェースでは有効となります。

- システムは system view に戻ります。それは、以下を意味します。
  - コマンドは system view と interface view のいずれでもサポートされています。
  - interface range view において、メンバインタフェースでの実行に失敗しましたが、system view で成功しました。
  - コマンドは、それ以降のメンバインタフェースで実行されませんでした。

display this コマンドで、それぞれのメンバインタフェースの interface view における設定を確認することができます。また、system view での設定が不要な場合、設定を取り消すために **undo** コマンドを使用してください。

インタフェースレンジの最初に指定したインタフェースの設定を確認する場合、interface range view で **display this** コマンドを実行します。

インタフェースレンジの設定を行う場合、以下のガイドラインに従ってください。

- インタフェースレンジで最初に指定するインタフェースを設定する前に、**interface** *interface-type interface-number* コマンドを使用してインタフェースの view に移行できることを確認してください。
- インタフェースレンジにアグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方を割り当てないでください。アグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方で実行すると、コマンドはアグリゲーションに失敗します。
- インタフェースレンジのインタフェースの最大数の制限の設定はありません。インタフェースレンジで多くのインタフェースを設定する場合、実行時間が長くなります。

例

GigabitEthernet 1/0/1 と VLAN-interface 2 をシャットダウンします。

<AP> system-view

[AP] interface range GigabitEthernet 1/0/1 Vlan-interface 2

[AP-if-range] shutdown

3.1.3 interface range name

Syntax

interface range name *name* [**interface** *interface-list*]

undo interface range name *name*

View

System view

定義済みユーザロール

network-admin

パラメータ

name: インタフェースレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

interface-list: インタフェースを指定します。半角スペースで区切り、24 までインタフェースを指定するか、インタフェースの範囲を指定します。インタフェースの範囲の形式は *interface-type interface-number* **to** *interface-type interface-number* です。*interface-type interface-number1* **to** *interface-type interface-number2* を指定したとき、*interface-number2* は *interface-number1* 以上の値にしてください。

説明

interface range name *name* **interface** *interface-list* コマンドはインタフェースレンジを作成し、インタフェースレンジの名前を設定し、interface range view に移行します。

interface パラメータを指定しない場合、指定された名前のインタフェースレンジの view に移行します。

undo interface range name コマンドは指定された名前のインタフェースレンジを削除します。

インタフェースレンジに名前を割り当てるために、コマンドを使用することができます。インタフェースレンジではなくインタフェースの名前を指定して interface range view に移行することができます。

interface range name コマンドで作成されたインタフェースレンジはカレントコンフィグレーションに保存され、メンバインタフェースを繰り返し使用することができます。

interface range view では、最初に指定したインタフェースでサポートされているコマンドのみ有効ですインタフェースレンジの最初に指定したインタフェースでサポートされるコマンドを表示する場合、interface range view に移行し、インタフェースのコマンドラインでクエスチョン（**?**）を入力します。

interface range view でコマンドを実行した後、以下のいずれかの状態が起こる可能性があります。

- システムは、エラーメッセージを表示し interface range view にとどまります。それは、メンバインタフェースで実行が失敗したことを意味します。
  - □ 最初のメンバインタフェースで失敗した場合、コマンドはどのメンバインタフェースでも実行されません。
  - □ 最初のメンバインタフェース以外で失敗した場合、コマンドは他のメンバインタフェースでは有効となります。
- システムは、system view に戻ります。それは、以下を意味します。
  - □ コマンドは system view と interface view のいずれでもサポートされています。
  - □ interface range view において、メンバインタフェースでの実行に失敗しましたが、system view で成功しました。
  - □ コマンドは、それ以降のメンバインタフェースで実行されませんでした。

display this コマンドで、それぞれのメンバインタフェースの interface view における設定を確認することができます。また、system view での設定が不要な場合、設定を取り消すために **undo** コマンドを使用してください。

インタフェースレンジの最初に指定したインタフェースの設定を確認する場合、interface range view で **display this** コマンドを実行します。

インタフェースレンジのメンバインタフェースを表示する場合、**display interface range** コマンドを使用します。

インタフェースレンジの設定を行う場合、以下のガイドラインに従ってください。

- インタフェースレンジで最初に指定するインタフェースを設定する前に、**interface** *interface-type interface-number* コマンドを使用してインタフェースの view に移行できることを確認してください。
- インタフェースレンジにアグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方を割り当てないでください。アグリゲートインタフェースとアグリゲートインタフェースのメンバインタフェースの両方で実行すると、コマンドはアグリゲーションに失敗します。
- インタフェースレンジのインタフェースの最大数の制限の設定はありません。インタフェースレンジで多くのインタフェースを設定する場合、実行時間が長くなります。
- インタフェースレンジの名前の最大数はシステムリソースによってのみ制限されます。インタフェースレンジの設定を保証するため、1000 個のインタフェースレンジの名前より少ない数にしてください。

例

インタフェースレンジ **myEthPort** に GigabitEthernet 1/0/1 を追加し、interface range view に移行します。

```
<AP> system-view
[AP] interface range name myEthPort interface gigabitethernet 1/0/1
[AP-if-range-myEthPort]
```

インタフェースレンジ **myEthPort** の view に移行します。

```
<AP> system-view
```

[AP] interface range name myEthPort

[AP-if-range-myEthPort]

関連コマンド

display interface range

QX-W610 アクセスポイント

コマンドマニュアル

04. ネットワーク

本マニュアルは以下に示す章で構成されています。

01-MAC アドレステーブル

02-VLAN

03-ループ検出

04-スパニングツリー

05- LLDP

06-Layer2 フォワーディング

07-ARP

08-IP アドレス

09-DHCP

10-DNS

11-NAT

12-IP パフォーマンスの最適化

13-スタティックルーティング

目次

このセクションのページは **4-x-x** です。

1 章 MAC アドレステーブル 1-1
1.1 MAC アドレステーブル設定コマンド 1-1
1.1.1 display mac-address 1-1
1.1.2 display mac-address aging-time 1-3
1.1.3 display mac-address mac-learning 1-4
1.1.4 display mac-address mac-move 1-5
1.1.5 mac-address (interface view) 1-6
1.1.6 mac-address (system view) 1-8
1.1.7 mac-address mac-learning enable 1-10
1.1.8 mac-address max-mac-count (interface view) 1-11
1.1.9 mac-address max-mac-count enable-forwarding (interface view) 1-13
1.1.10 mac-address notification mac-move 1-14
1.1.11 mac-address notification mac-move suppression (interface view) 1-15
1.1.12 mac-address notification mac-move suppression (system view) 1-16
1.1.13 mac-address timer 1-17
1.1.14 snmp-agent trap enable mac-address 1-18

1章 MAC アドレステーブル

1.1 MACアドレステーブル設定コマンド

1.1.1 display mac-address

Syntax

display mac-address [*mac-address* [**vlan** *vlan-id*] | [[**dynamic** | **static**] [**interface** *interface-type interface-number*] | **blackhole**] [**vlan** *vlan-id*] [**count**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address: MAC アドレスを指定します。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: VLAN ID を指定します。設定範囲は 1～4094 です。

dynamic: ダイナミック MAC アドレスエントリを表示します。

static: スタティック MAC アドレスエントリを表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

blackhole: ブラックホール MAC アドレスエントリを表示します。

count: コマンドで指定したすべてのエントリに一致する MAC アドレスエントリ数のみを表示します。MAC アドレスエントリの詳細は表示されません。たとえば、VLAN 20 のダイナミックエントリ数を表示する場合、**display mac-address vlan** *20* **dynamic count** コマンドを使用します。エントリの属性が指定されない場合、MAC アドレステーブルのエントリ数を表示します。**count** を指定しない場合、指定された MAC アドレスエントリの詳細情報を表示します。

説明

display mac-address コマンドは MAC アドレスエントリを表示します。

MAC アドレスエントリは宛先 MAC アドレス、出力インタフェース、VLAN ID が含まれます。

パラメータを指定しない場合、すべての MAC アドレスエントリを表示します。

アグリゲートインタフェースに少なくとも 1 つの Selected メンバポートがある場合、アグリゲートインタフェースのダイナミック MAC アドレスエントリのみ表示します。

例

VLAN 100 の MAC アドレスエントリを表示します。

<AP> display mac-address vlan 100

```
MAC Address      VLAN ID    State          Port/NickName          Aging
0033-0033-0033   100        Blackhole       N/A                   N
0000-0000-0002   100        Static         GE1/0/3                N
0000-0000-5829   100        Learned        GE1/0/4                Y
```

MAC アドレスエントリ数を表示します。

<AP> display mac-address count

```
1 mac address(es) found.
```

表 1-1 コマンド出力

フィールド	説明
VLAN ID	MACアドレスエントリが所属する出力インタフェースのVLAN IDです。
State	MACアドレスエントリの状態です。 ● **Static**—スタティックMACアドレスエントリです。 ● **Learned**—ダイナミックMACアドレスエントリです。ダイナミックエントリは自動あるいは手動で設定されたものがあります。 ● **Blackhole**—ブラックホールMACアドレスエントリです。
Port/NickName	MACアドレスに関連づけられるパケットの出力インタフェースです。ブラックホールMACアドレスエントリの場合、**N/A**と表示されます。 16進数（0x12abなど）が表示されている場合は、パケットがTRILLネットワークから出るRBを示します。ニックネームは表示できますが、設定することはできません。
Aging	エントリがエージングアウト可能かどうかを示します。 ● **Y**—エントリはエージングアウト可能です。 ● **N**—エントリはエージングアウトできません。
mac address(es) found	MACアドレスエントリに一致する数です。

関連コマンド

- **mac-address**
- **mac-address timer**

1.1.2 display mac-address aging-time

Syntax

display mac-address aging-time

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mac-address aging-time コマンドはダイナミック MAC アドレスエントリのエージングタイマを表示します。

例

ダイナミック MAC アドレスエントリのエージングタイマを表示します。

<AP> display mac-address aging-time

```
MAC address aging time: 300s.
```

関連コマンド

mac-address timer

1.1.3 display mac-address mac-learning

Syntax

display mac-address mac-learning [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

インタフェースを指定しない場合、グローバル MAC アドレスの学習状態とすべてのインタフェースの MAC アドレスの学習状態を表示します。

説明

display mac-address mac-learning コマンドはグローバル MAC アドレスの学習状態と指定された、あるいはすべてのインタフェースの MAC アドレスの学習状態を表示します。

例

グローバル MAC アドレスの学習状態とすべてのインタフェースの MAC アドレスの学習状態を表示します。

<AP> display mac-address mac-learning

```
Global MAC address learning status: Enabled.

Port                    Learning Status
GE1/0/1                 Enabled
```

表 1-2 コマンド出力

フィールド	説明
Global MAC address learning status	グローバルMACアドレスの学習状態です。 ● 有効です。 ● 無効です。
Learning Status	インタフェースのMACアドレスの学習状態を表示します。 ● 有効です。 ● 無効です。

関連コマンド

mac-address mac-learning enable

1.1.4 display mac-address mac-move

Syntax

display mac-address mac-move

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display mac-address mac-move コマンドは装置が起動した後、MAC アドレスの移動記録を表示します。

指定された 2 つのインタフェース間で MAC アドレスの移動が発生したとき、ネットワークでレイヤ 2 でのループが発生する可能性があります。ループを検出し、位置を特定するために MAC アドレスの移動記録を表示することができます。

- MAC アドレスの移動記録では、同一 MAC アドレス、VLAN、送信元ポート、現在のポートの記録が 1 つの記録として認識されます。
- デバイスは最大 20 の MAC アドレス移動記録を保存できます。MAC アドレス移動記録の数が 20 を超えると、最新のレコードは最後の MAC アドレスの移動時間に基づいて最も古い記録に上書きします。

例

MAC アドレス移動記録を表示します。

<AP> display mac-address mac-move

```
MAC address    VLAN Current port   Source port    Last time          Times
0000-0001-001 1    GE1/0/3       GE1/0/3       2013-05-20 13:42:22 13
0000-0001-001 1    GE1/0/4       GE1/0/4       2013-05-20 13:42:21 12
---  4 MAC address moving records found  ---
```

表 1-3 コマンド出力

フィールド	説明
VLAN	MACアドレスエントリが属している出力インタフェースのVLANです。
Current port	MACアドレスが移動したインタフェースです。
Source port	MACアドレスが移動する前のインタフェースです。
Last time	最後にMACアドレスが移動したときの時間です。
Times	装置が起動したのち、MACアドレスが移動した数です。 新しいMACアドレスの移動が、MACアドレスの記録として、同じMACアドレス、VLAN、現在のポート、送信元ポートのフィールドを持っていたとき、MACアドレスを記録するため、MACアドレスの移動した数は1つずつ増加します。

関連コマンド

mac-address notification mac-move

1.1.5 mac-address (interface view)

Syntax

mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

デフォルト

設定なし

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

dynamic: ダイナミック MAC アドレスエントリを指定します。

static: スタティック MAC アドレスエントリを指定します。

mac-address: MAC アドレスを指定します。マルチキャスト MAC アドレスとすべてが 0 の MAC アドレスを除きます。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: 指定されたインタフェースが所属する既存の VLAN ID を指定します。設定範囲は 1〜4094 です。

説明

mac-address コマンドはインタフェースの MAC アドレスエントリを追加あるいは修正します。

undo mac-address コマンドはインタフェースの MAC アドレスエントリを削除します。

一般的に、装置は自動で各インタフェースの受信フレームの送信元 MAC アドレスによって学習された MAC アドレステーブルを構築します。しかし、手動でスタティック MAC アドレスエントリを設定することができます。手動で設定されたスタティック MAC アドレスエントリはダイナミック MAC アドレスエントリよりも優先されます。インタフェースに接続されたユーザの装置のセキュリティを向上するため、ユーザの装置をインタフェースに関連づけるため、スタティックエントリを設定します。ユーザの装置（たとえばホスト A）のフレームは常にインタフェースから送信されます。ホスト A の偽の MAC アドレスを使用するほかのホストはホスト A からのフレームを取得することができません。

MAC アドレスエントリの設定は、設定を保存しないと、再起動により削除されます。ただしダイナミック MAC アドレスエントリは設定の保存に関わらず、再起動により削除されます。

例

VLAN 2 に所属する GigabitEthernet 1/0/1 に MAC アドレス 000f-e201-0101 のスタティック MAC アドレスエントリを追加します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] mac-address static 000f-e201-0101 vlan 2

VLAN 1 に所属するアグリゲートインタフェース Bridge-Aggregation 1/0/1 に MAC アドレス 000f-e201-0101 のスタティック MAC アドレスエントリを追加します。

<AP> system-view

[AP] interface bridge-aggregation 1

[AP-Bridge-Aggregation1] mac-address static 000f-e201-0102 vlan 1

関連コマンド

- **display mac-address**
- **mac-address (system view)**

1.1.6 mac-address (system view)

Syntax

mac-address static *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

mac-address blackhole *mac-address* **vlan** *vlan-id*

undo mac-address [[**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**blackhole** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**static**] **interface** *interface-type interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

static: スタティック MAC アドレスエントリを指定します。

blackhole: ブラックホール MAC アドレスエントリを指定します。宛先 MAC アドレスがブラックホール MAC アドレスに一致している場合、パケットは廃棄されます。

mac-address: MAC アドレスを指定します。マルチキャスト MAC アドレスとすべてが 0 の MAC アドレスを除きます。形式は H-H-H です。H の先頭から 0 が続く場合は省略できます。たとえば、000f-00e2-0001 は、f-e2-1 と省略できます。

vlan *vlan-id*: 指定されたインタフェースが所属する既存の VLAN ID を指定します。設定範囲は 1～4094 です。

interface *interface-type interface-number*: 出力インタフェースのタイプと番号を指定します。

説明

mac-address コマンドは MAC アドレスエントリを追加あるいは修正します。

undo mac-address コマンドは 1 つあるいはすべての MAC アドレスエントリを削除します。

以下のタイプの MAC アドレスエントリを設定することができます。

- スタティックエントリ

手動で設定されたスタティックエントリはダイナミックエントリよりも優先します。インタフェースに接続されたデバイスのセキュリティを向上するため、インタフェースに

割り当てるデバイスのスタティックエントリを設定します。デバイス向け（たとえば、Host A）のフレームは常にインタフェースに送信されます。Host A の MAC アドレスに偽造させた MAC アドレスを使用するほかのホストは Host A 向けのフレームを受信することができません。

- ブラックホールエントリ

指定された宛先 MAC アドレスのフレームを廃棄するため、ブラックホールエントリを設定することができます。

スタティックあるいはブラックホール MAC アドレスエントリはダイナミック MAC アドレスエントリに上書きすることができます。ダイナミック MAC アドレスエントリはスタティックあるいはブラックホール MAC アドレスエントリに上書きすることはできません。

パラメータを指定しないで **undo mac-address** コマンドを実行した場合、すべてのユニキャスト MAC アドレスエントリを削除します。

指定した VLAN のすべての MAC アドレスエントリを削除することができます。また特定のタイプ（ダイナミック、スタティック、ブラックホール）の MAC アドレスエントリのみを削除することができます。1 つのインタフェースのみを選択することで、対応する MAC アドレスエントリを削除します。

MAC アドレスエントリの設定は、設定を保存しないと、再起動により削除されます。ただしダイナミック MAC アドレスエントリは設定の保存に関わらず、再起動により削除されます。

例

MAC アドレス 000f-e201-0101 のスタティックエントリを追加します。次に、この MAC アドレスを宛先とするすべてのフレームが VLAN 2 に所属する GigabitEthernet 1/0/1 から送信します。

<AP> system-view

[AP] mac-address static 000f-e201-0101 interface gigabitethernet 1/0/1 vlan 2

関連コマンド

- **display mac-address**
- **mac-address (interface view)**

1.1.7 mac-address mac-learning enable

Syntax

mac-address mac-learning enable

undo mac-address mac-learning enable

デフォルト

有効

View

System view

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-address mac-learning enable コマンドはグローバル、インタフェースで MAC アドレスの学習を有効にします。

undo mac-address mac-learning enable コマンドはグローバル、インタフェースで MAC アドレスの学習を無効にします。

MAC アドレステーブルが一杯になることを防ぐため、MAC アドレステーブルの学習を無効にすることができます。

たとえば、攻撃者からの異なる送信元 MAC アドレスの大量のパケットを学習しないように、以下のガイドラインに従い、装置で MAC アドレスの学習を無効にすることができます。

- インタフェースごとに MAC アドレスの学習を無効にすることができます。グローバルで MAC アドレスの学習を無効にした場合、すべてのインタフェースで MAC アドレスの学習が無効になります。装置は MAC アドレスの学習を停止し、ダイナミックに MAC アドレステーブルのアップデートを行うことができません。
- MAC アドレスの学習を無効にすると、ブロードキャストストームが発生する可能性あるため、インタフェースで MAC アドレスの学習を無効にしたのち、ブロードキャストストームの抑制を行ってください。ブロードキャストストームの抑制の詳細は、オペレーションマニュアルのセクション 3 *インタフェース　"Ethernet"* を参照してください。
- グローバルで MAC アドレスの学習を有効にし、インタフェースで MAC アドレスの学習を無効にすることができます。
- MAC アドレスの学習を無効にしたとき、装置はインタフェースにある既存のダイナミック MAC アドレスエントリを即座に削除します。

例

グローバルで MAC アドレスの学習を無効にします。

<AP> system-view

[AP] undo mac-address mac-learning enable

GigabitEthernet 1/0/1 で MAC アドレスの学習を無効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] undo mac-address mac-learning enable

アグリゲートインタフェース Bridge-Aggregation 1 で MAC アドレスの学習を無効にします。

<AP> system-view

[AP] interface bridge-aggregation 1

[AP-Bridge-Aggregation1] undo mac-address mac-learning enable

関連コマンド

display mac-address mac-learning

1.1.8 mac-address max-mac-count (interface view)

Syntax

mac-address max-mac-count *count*

undo mac-address max-mac-count

デフォルト

2048

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

count: インタフェースで学習できる MAC アドレスの最大数を指定します。値の範囲は 0～2048 です。引数が 0 に設定されている場合、インタフェースは MAC アドレスの学習が行われません。

説明

mac-address max-mac-count コマンドはインタフェースで学習できる MAC アドレスの最大数を設定します。

undo mac-address max-mac-count コマンドはデフォルトに戻します。

mac-address max-mac-count コマンドは MAC アドレステーブルのサイズを制限するため、MAC アドレスエントリ数を制限します。

MAC アドレステーブルが大きくなるとフォワーディングの性能に影響します。インタフェースで学習した MAC アドレスの数が上限に達した場合、インタフェースは MAC アドレスエントリの学習を停止します。

例

GigabitEthernet 1/0/1 で学習できる MAC アドレスエントリの最大数を 200 に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] mac-address max-mac-count 200

関連コマンド

- **mac-address**
- **mac-address max-mac-count enable-forwarding (interface view)**

1.1.9 mac-address max-mac-count enable-forwarding (interface view)

Syntax

mac-address max-mac-count enable-forwarding

undo mac-address max-mac-count enable-forwarding

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-address max-mac-count enable-forwarding コマンドはインタフェースで学習できる MAC アドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを有効にします。

undo mac-address max-mac-count enable-forwarding コマンドはインタフェースで学習できる MAC アドレスの数が制限に到達したのち、インタフェースで受信された未知のフレームを装置が転送することを無効にします。

未知のフレームとは、送信元 MAC アドレスが MAC アドレステーブルにないフレームを指します。

例

MAC アドレスエントリを最大 200 まで学習できるように GigabitEthernet 1/0/1 を設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] mac-address max-mac-count 200

GigabitEthernet 1/0/1 で学習できる MAC アドレスの数が制限に到達したのち、GigabitEthernet 1/0/1 で受信された未知のフレームを装置が転送することを無効にします。

[AP-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding

関連コマンド

- **mac-address**
- **mac-address max-mac-count (interface view)**

1.1.10 mac-address notification mac-move

Syntax

mac-address notification mac-move [**interval** *interval-value*]

undo mac-address notification mac-move

デフォルト

MAC アドレスの検出は無効です。MAC アドレスの移動の検出間隔は 1 分です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: MAC アドレスの移動の検出間隔を指定します。設定範囲は 1～60 分です。パラメータを指定しない場合、デフォルトで 1 分が指定されます。

説明

mac-address notification mac-move コマンドは MAC アドレスの移動を通知することを有効にし、MAC アドレスの検出間隔を指定します。

undo mac-address notification mac-move コマンドはデフォルトに戻します。

MAC アドレスの移動の通知を有効にした際、システムが MAC アドレスの移動を検出したとき、MAC アドレスが移動したログを表示します。各 MAC アドレスの移動ログは以下の情報が含まれます。

- MAC アドレス
- MAC アドレスエントリの VLAN ID
- MAC アドレスの移動元のポートと移動先のポート
- MAC アドレスの検出間隔以内に MAC アドレスが移動した数

MAC アドレスは 1 つの MAC アドレスの移動記録のみ保持することができます。

このコマンドを実行した後、システムは Information Center に syslog メッセージのみを送信します。**snmp-agent trap enable mac-address** コマンドが有効である場合、装置の SNMP モジュールに SNMP 情報を送信します。

検出間隔内で、装置は最大 20 個の MAC アドレスの移動を記録できます。制限値を超過すると、装置は他の MAC アドレスの MAC アドレス移動レコードを削除します。次の検出間隔では、新しい MAC アドレスの移動記録は、前の検出間隔で生成された最も古いものに上書きします。

例

MAC アドレスの移動を通知することを有効にします。

<AP> system-view

[AP] mac-address notification mac-move

[AP]

```
%May 14 17:16:45:688 2013 Sysname MAC/4/MAC_FLAPPING: MAC address 0000-0012-0034
in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times
```

出力は以下のこと示します。

- MAC アドレス 0000-0012-0034 の VLAN ID は 500 です。
- MAC アドレスは GigabitEthernet 1/0/1 から GigabitEthernet 1/0/2 に移動しました。
- MAC アドレスは最新の 1 分以内に 1 回移動しました。

関連コマンド

display mac-address mac-move

1.1.11 mac-address notification mac-move suppression (interface view)

Syntax

mac-address notification mac-move suppression

undo mac-address notification mac-move suppression

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

mac-address notification mac-move suppression コマンドは MAC アドレスの移動の抑制機能を有効にします。

undo mac-address notification mac-move suppression コマンドはデフォルトに戻します。

説明

MAC アドレスの検出期間以内に、指定した抑制しきい値より多くの MAC アドレスがインタフェースから移動したとき、インタフェースをシャットダウンします。インタフェースを UP 状態にする場合、手動で **shutdown** コマンドを実行し、**undo shutdown** コマ

ンドを実行する必要があります。抑制間隔後、インタフェースは自動で UP 状態となります。

MAC アドレスの移動の抑制機能がインタフェースをシャットダウンするとき、システムは Information Center モジュールに syslog メッセージのみを送信します。**snmp-agent trap enable mac-address** コマンドが有効である場合、装置の SNMP モジュールに SNMP 情報を送信します。

例

GigabitEthernet 1/0/1 で MAC アドレスの移動の抑制機能を有効にします。

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] mac-address notification mac-move suppression

関連コマンド

mac-address notification mac-move suppression (system view)

1.1.12 mac-address notification mac-move suppression (system view)

Syntax

mac-address notification mac-move suppression { **interval** *interval-value* | **threshold** *threshold-value* }

undo mac-address notification mac-move suppression { **interval** | **threshold** }

デフォルト

MAC アドレスの抑制間隔は 30 秒です。MAC アドレスのしきい値は 3 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: MAC アドレスの抑制間隔を指定します。設定範囲は 30～86400 秒です。パラメータを指定しない場合、30 秒が指定されます。

threshold *threshold-value*: 検出間隔内に送信元のインタフェースから移動する MAC アドレスのしきい値を設定します。設定範囲は 0～1024 です。パラメータを指定しない場合、3 が指定されます。

説明

mac-address notification mac-move suppression コマンドは MAC アドレスの抑制間隔、あるいは MAC アドレス移動のしきい値を設定します。

undo mac-address notification mac-move suppression コマンドはデフォルトに戻します。

インタフェースでコマンドを適用する場合、MAC アドレスの移動の抑制機能を有効にする必要があります。

MAC アドレスの抑制間隔あるいは MAC アドレスのしきい値を複数回設定した場合、最後に行った設定が適用されます。抑制間隔の設定は MAC アドレス移動のしきい値の設定と独立しています。

例

MAC アドレスの抑制間隔を 40 秒に設定し、MAC アドレス移動のしきい値を 1 に設定します。

<AP> system-view

[AP] mac-address notification mac-move suppression interval 40

[AP] mac-address notification mac-move suppression threshold 1

関連コマンド

mac-address notification mac-move suppression (interface view)

1.1.13 mac-address timer

Syntax

mac-address timer { **aging** *seconds* | **no-aging** }

undo mac-address timer

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

aging *seconds*: ダイナミック MAC アドレスエントリのエージングタイマ（秒単位）を設定します。範囲は 10～630 です。

no-aging: ダイナミック MAC アドレスエントリをエージアウトしないように設定します。

説明

mac-address timer コマンドはダイナミック MAC アドレスエントリのエージングタイマを設定します。

undo mac-address timer コマンドはデフォルトに戻します。

適切にエージングタイマを設定するために、以下のガイドラインに従ってください。

- エージング間隔が長いと、エージングタイマが終了したエントリを MAC アドレステーブルに残す可能性があり、最新のネットワークの変化に対応できなくなる可能性があります。
- エージング間隔が短いと、有効なエントリを削除してしまい、装置のパフォーマンスに影響を及ぼす不要なブロードキャストを送信する結果になる可能性があります。

例

ダイナミック MAC アドレスエントリのエージングタイマを 500 秒に設定します。

<AP> system-view

[AP] mac-address timer aging 500

関連コマンド

display mac-address aging-time

1.1.14 snmp-agent trap enable mac-address

Syntax

snmp-agent trap enable mac-address [mac-move]

undo snmp-agent trap enable mac-address [mac-move]

デフォルト

MAC アドレス テーブルに対して SNMP 通知が有効になっています。

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-move: MAC アドレス テーブルの MAC アドレスの移動に関する通知を指定します。このキーワードを指定しない場合、コマンドは MAC アドレス テーブルのすべてのタイプの SNMP 通知を有効にします。

説明

snmp-agent trap enable mac-address を使用して、MAC アドレス テーブルの SNMP 通知を有効にします。

undo snmp-agent trap enable mac-address を使用して、MAC アドレス テーブルの SNMP 通知を無効にします。

重要な MAC アドレス移動イベントを NMS に報告するには、MAC アドレス テーブルの SNMP 通知を有効にします。MAC アドレス移動イベント通知が正しく送信されるようにするには、デバイスで SNMP を設定する必要もあります。MAC アドレス テーブルの SNMP 通知が無効になっている場合、デバイスは生成されたログをインフォメーション センターに送信します。ログを表示するには、インフォメーション・センターでログの宛先と出力ルール構成を構成します。MAC アドレス テーブルは、MAC アドレスの移動に関する SNMP 通知のみをサポートします。MAC アドレスの移動に関する SNMP 通知を有効または無効にすると、MAC アドレス テーブルのすべてのタイプの SNMP 通知が有効または無効になります。

例

MAC アドレス テーブルの MAC アドレスの移動に関する SNMP 通知を無効にします。

```
<AP> system-view
[AP] undo snmp-agent trap enable mac-address mac-move
```

関連コマンド

mac-address notification mac-move

目次

このセクションのページは **4-x-x** です。

2 章 VLAN 2-1
2.1 ベーシック VLAN 設定コマンド 2-1
2.1.1 description 2-1
2.1.2 display interface vlan-interface 2-3
2.1.3 display vlan 2-8
2.1.4 display vlan brief 2-10
2.1.5 interface vlan-interface 2-11
2.1.6 name 2-12
2.1.7 reset counters interface vlan-interface 2-13
2.1.8 shutdown 2-14
2.1.9 vlan 2-16
2.2 ポートベース VLAN 設定コマンド 2-18
2.2.1 display port 2-18
2.2.2 port 2-20
2.2.3 port access vlan 2-21
2.2.4 port hybrid pvid 2-22
2.2.5 port hybrid vlan 2-24
2.2.6 port link-type 2-26
2.2.7 port trunk permit vlan 2-27
2.2.8 port trunk pvid 2-29

2章 VLAN

2.1 ベーシックVLAN設定コマンド

2.1.1 description

Syntax

description *text*

undo description

デフォルト

VLAN の説明は VLAN *vlan-id* です。*vlan-id* は VLAN の ID です。たとえば、VLAN 100 の VLAN の説明は VLAN 0100 です。

VLAN インタフェースの説明はインタフェースの名前です。たとえば Vlan-interface1 Interface です。

View

VLAN view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

text: VLAN あるいは VLAN インタフェースの説明を指定します。設定範囲は 1～255 です。文字列には、大文字と小文字を区別する文字、数字、特殊記号（表 3-1 を参照）、スペース、その他の Unicode 文字と記号を含めることができます。

表 2-1 特殊記号

名前	記号
チルダ	~
エクスクラメーションマーク	!
アットマーク	@
シャープ	#
ダラーマーク	$
パーセント	%
キャロット	^
アンパサンド	&
アスタリスク	*

名前	記号
左波括弧	{
右波括弧	}
左丸括弧	(
右丸括弧	)
左角括弧	[
右角括弧	]
左アングルブラケット	<
右アングルブラケット	>
ハイフン	-
アンダーライン	_
＋マーク	+
イコールマーク	=
バーティカルバー	|
バックスラッシュ	¥
コロン	:
セミコロン	;
ダブルクォーテーション	"
アポストロフィー	'
コンマ	,
ドット	.
スラッシュ	/

説明

description コマンドは VLAN あるいは VLAN インタフェースの説明を指定します。

undo description コマンドはデフォルトに戻します。

VLAN あるいは VLAN インタフェースの機能あるいは説明を設定することができます。

装置で多くの VLAN あるいは VLAN インタフェースを識別するのに役立ちます。

例

VLAN 2 の説明を sales-private に設定します。

<AP> system-view

[AP] vlan 2

[AP-vlan2] description sales-private

VLAN インタフェース 2 の説明を linktoPC56 に設定します。

<AP> system-view

[AP] vlan 2

[AP-vlan2] quit

[AP] interface vlan-interface 2

[AP-Vlan-interface2] description linktoPC56

関連コマンド

- **display interface vlan-interface**
- **display vlan**

2.1.2 display interface vlan-interface

Syntax

display interface [**vlan-interface** [*interface-number*] [**brief** [**description** | **down**]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-interface *interface-number*: VLAN インタフェース番号を指定します。指定しない場合、すべての VLAN インタフェースの情報を表示します。インタフェースを指定せずに vlan-interface キーワードを指定した場合、コマンドはすべての VLAN インタフェースに関する情報を表示します。

brief: インタフェースの概要情報を表示します。指定しない場合、VLAN インタフェースの詳細情報を表示します。

description: 完全なインタフェースの説明を表示します。指定しない場合、説明の最初の 27 文字のみを表示します。

down: down 状態の VLAN インタフェース、原因を表示します。指定しない場合、すべての状態の VLAN インタフェースの情報を表示します。

説明

display interface vlan-interface コマンドは VLAN インタフェースの情報を表示します。

例

VLAN インタフェース 2 の情報を表示します。

<AP> display interface vlan-interface 2

```
Vlan-interface2
Current state: DOWN
Line protocol state: DOWN
```

```
Description: Vlan-interface2 Interface
Bandwidth: 100000kbps
Maximum transmission unit: 1500
Internet protocol processing : Disabled
IP packet frame type: PKTFMT_ETHNT_2, hardware address: 000f-e249-8050
IPv6 packet frame type: PKTFMT_ETHNT_2, hardware address: 000f-e249-8050
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 0 packets, 0 bytes, 0 drops
Output: 0 packets, 0 bytes, 0 drops
```

VLAN インタフェース 2 の概要情報を表示します。

<AP> display interface vlan-interface 2 brief

```
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP       Description
Vlan2                DOWN DOWN     --
```

表 2-2 コマンド出力

フィールド	説明
Vlan-interface2	VLANインタフェース名です。
Current state	VLANインタフェースの物理状態です。 • **DOWN (Administratively)**–**shutdown**コマンドでVLANインタフェースがシャットダウンしています。インタフェースは運用上においてdownしています。 • **DOWN**–**shutdown**コマンドでVLANインタフェースがシャットダウンしていませんが、物理的にdownしています。VLANインタフェースのVLANはup状態の物理ポートがありません。ポートが物理的に接続されていない、あるいはリンクに失敗している可能性があります。 • **UP**–VLANインタフェースが運用上も物理的にも起動している状態です。

フィールド	説明
Line protocol state	VLANインタフェースのプロトコルリンクレイヤの状態です。 ● **DOWN**–VLANインタフェースがプロトコルリンクレイヤでdownしています。 ● **UP**–VLANインタフェースがプロトコルリンクレイヤでupしています。
Description	VLANインタフェースの一部または全部の説明です。 ● **display interface brief**コマンドで**description**キーワードを指定しない場合、このフィールドにはインタフェースの説明の最初の27文字が表示されます。 ● **display interface brief**コマンドで**description**キーワードを指定した場合、このフィールドには完全なインタフェースの説明が表示されます。
Bandwidth	VLANインタフェースの予期された帯域幅です。
Maximum Transmission Unit	VLANインタフェースのMTUです。
Internet protocol processing : Disabled	VLANインタフェースにIPアドレスが設定されておらず、IPパケットの処理できません。
Internet address: ip-address/mask-length (Type)	インタフェースのIPアドレスと、かっこ内のアドレスのタイプです。 ● **Primary**—手動で設定されたプライマリIPアドレスです。 ● **Sub**—手動で設定されたセカンダリIPアドレスです。インタフェースにプライマリIPアドレスとセカンダリIPアドレスの両方がある場合は、プライマリIPアドレスが表示されます。インタフェースにセカンダリIPアドレスしかない場合は、最も小さいセカンダリIPアドレスが表示されます。 ● **DHCP-allocated**—DHCPによって割り当てられたIPアドレス。詳細については、コマンドマニュアルのセクション4 *"DHCP"*を参照してください。 ● **BOOTP-allocated**—BOOTPによって割り当てられたIPアドレスです。 ● **PPP-negotiated**—PPPネゴシエーション中にPPPサーバによって割り当てられるIPアドレスです。 ● **Unnumbered**—別のインタフェースから借用したIPアドレスです。
IP packet frame type	IPv4の送信フレームタイプです。
hardware address	VLANインタフェースに対応するMACアドレスです。

フィールド	説明
Last clearing of counters	インタフェースで**reset counters interface**コマンドを最後に使用した時間です。 **Never**は装置が起動してから**reset counters interface**コマンドを一度も使用していないことを示します。
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec	過去300秒以内の平均送受信トラフィックです。単位はバイト/秒、bps、ppsです。
Input: 0 packets, 0 bytes, 0 drops	インタフェースで受信されたパケットの総数、パケットサイズと廃棄されたパケット数です。パケットサイズの単位はバイトです。
Output: 0 packets, 0 bytes, 0 drops	インタフェースで送信されたパケットの総数、パケットサイズと廃棄されたパケット数です。パケットサイズの単位はバイトです。
Last 300 seconds input rate: 0 packets/sec, 0 bytes/sec	過去300秒間の平均受信トラフィックレート (ppsおよびbps) です。ハイフン(-)は、統計項目がサポートされていないことを示します。
Last 300 seconds output rate: 0 packets/sec, 0 bytes/sec	過去300秒間の平均発信トラフィックレート (ppsおよびbps単位) です。ハイフン(-)は、統計項目がサポートされていないことを示します。
Input: 0 packets, 0 bytes	インタフェースの受信トラフィック統計情報 (パケット数およびバイト数) 。ハイフン(-)は、統計項目がサポートされていないことを示します。
Output: 0 packets, 0 bytes	インタフェースの送信トラフィックの統計情報 (パケット数およびバイト数) 。ハイフン(-)は、統計項目がサポートされていないことを示します。
Brief information on interfaces in route mode	レイヤ3インタフェースの概要情報です。
Interface	省略したインタフェース名です。
Link	インタフェースの物理リンク状態です。 • **UP**–リンクがupです。 • **DOWN**–リンクが物理的にdownしています。 • **ADM**–リンクが運用上でシャットダウンしています。物理状態を回復するために、**undo shutdown**コマンドを実行します。 • **Stby**–インタフェースがバックアップインタフェースとして動作します。

フィールド	説明
Protocol	インタフェースのリンクレイヤの状態です。 • **UP**－インタフェースのリンクがupです。 • **DOWN**－インタフェースのリンクがdownです。 • **UP(s)**–インタフェースのリンクがオンデマンドリンクあるいは準備ができていない状態です。ここで（**s**）はスプーフィングのフラグを示します。
Primary IP	インタフェースのプライマリIPアドレスです。

関連コマンド

reset counters interface vlan-interface

2.1.3 display vlan

Syntax

display vlan [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **reserved** | **static**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan-id1: VLAN ID で指定された VLAN の情報を表示します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN ID の範囲を指定します。*vlan-id1* と *vlan-id2* の設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* よりも大きい値にする必要があります。

all: 作成されたすべての VLAN の情報を表示します。

dynamic: ダイナミック VLAN の番号と各ダイナミック VLAN の ID を表示します。ダイナミック VLAN は RADIUS サーバによって作成されます。

reserved: 保持する VLAN を指定します。プロトコルモジュールは、機能の実装に従って保持される VLAN を決定します。保持された VLAN は、プロトコルモジュールのサービスを提供します。保持された VLAN は設定できません。

static: スタティック VLAN 番号と各スタティック VLAN の ID を表示します。スタティック VLAN は手動で作成されます。

説明

display vlan コマンドは VLAN 情報を表示します。

例

VLAN 2 の情報を表示します。

<AP> display vlan 2

```
VLAN ID: 2
VLAN type: Static
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports:  None
Untagged ports:
  GigabitEthernet1/0/1
```

VLAN 3 の情報を表示します。

<AP> display vlan 3

```
VLAN ID: 3
VLAN type: static
Route interface: Configured
IPv4 address: 1.1.1.1
IPv4 subnet mask: 255.255.255.0
Description: VLAN 0003
Name: VLAN 0003
Tagged ports:  None
Untagged ports: None
```

表 2-3 コマンド出力

フィールド	説明
VLAN type	VLANタイプです。スタティックあるいはダイナミックがあります。
Route interface	VLANインタフェースが設定されているかどうかを示します。 ● **Not configured**－設定されていません。 ● **Configured**－設定されています。
Description	VLANの説明です。
Name	VLANに設定された名前です。
IP address	VLANインタフェースのプライマリIPv4アドレスです。このフィールドはVLANインタフェースにIPv4アドレスが設定されている場合のみ表示されます。セカンダリIPアドレスが存在する場合、以下のいずれかの方法で表示することができます。 ● **display interface vlan-interface**コマンドを使用します。 ● VLAN interface viewで**display this**コマンドを使用します。
Subnet mask	プライマリIPアドレスのサブネットマスクです。このフィールドはVLANインタフェースにIPアドレスが設定されている場合のみ表示されます。
Tagged ports	タグ付きVLANパケットを通すポートです。
Untagged ports	タグなしVLANパケットを通すポートです。

関連コマンド

vlan

2.1.4 display vlan brief

Syntax

display vlan brief

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display vlan brief コマンドは VLAN の概要情報を表示します。

例

VLAN の概要情報を表示します。

<AP> display vlan brief

```
Brief information about all VLANs:
Supported Minimum VLAN ID: 1
Supported Maximum VLAN ID: 4094
Default VLAN ID: 1
VLAN ID   Name                          Port
1         VLAN 0001                     GE1/0/1
2         VLAN 0002
3         VLAN 0003
```

表 2-4 コマンド出力

フィールド	説明
Default VLAN ID	システムのデフォルトVLAN IDです。
Name	VLAN名です。
Port	VLANを通してパケットを許可するポートです。

2.1.5 interface vlan-interface

Syntax

interface vlan-interface *interface-number*

undo interface vlan-interface *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: VLAN インタフェース番号を指定します。設定範囲は 1～4094 です。

サポートされる VLAN インタフェースの最大数は 48 です。

説明

interface vlan-interface コマンドは VLAN インタフェースを作成し、作成された VLAN インタフェースの view に移行あるいは既存の VLAN インタフェースの view に移行します。

undo interface vlan-interface コマンドは VLAN インタフェースを削除します。

VLAN インタフェースを作成する前に、VLAN を作成してください。

例

VLAN インタフェース 2 を作成し、作成された VLAN インタフェースの view に移行します。

<AP> system-view

[AP] vlan 2

[AP-vlan2] quit

[AP] interface vlan-interface 2

[AP-Vlan-interface2]

関連コマンド

display interface vlan-interface

2.1.6 name

Syntax

name *text*

undo name

デフォルト

デフォルトの VLAN 名は VLAN *vlan-id* です。*vlan-id* は 4 桁の VLAN の ID です。ID が 4 桁よりも少ない場合、先頭に 0 が追加されます。たとえば、VLAN 100 の VLAN 名は VLAN 0100 です。

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

text: VLAN 名を指定します。設定範囲は 1～32 です。文字列には、大文字と小文字を区別する文字、数字、特殊記号（表 3-1 を参照してください。）、スペース、その他の Unicode 文字と記号を含めることができます。

説明

name コマンドは VLAN の名前を設定します。

undo name コマンドは VLAN の名前をデフォルトに戻します。

装置に 802.1X または MAC アドレス認証の設定が行われる場合、VLAN ID または VLAN 名を使用して許可 VLAN を指定することができます。VLAN の数が非常に多い場合、識別するために VLAN 名を使用します。

例

VLAN 2 の名前を test vlan として設定します。

<AP> system-view

[AP] vlan 2

[AP-vlan2] name test vlan

関連コマンド

display vlan

2.1.7 reset counters interface vlan-interface

Syntax

reset counters interface vlan-interface [*interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

vlan-interface *interface-number*: VLAN インタフェース番号を指定します。

説明

reset counters interface vlan-interface コマンドは VLAN インタフェースの統計情報を削除します。

一定期間、トラフィックの統計情報を収集する場合、以前に収集された統計情報の履歴を削除し、このコマンドを使用します。

- **interface-number** 引数を指定しない場合、このコマンドはすべての VLAN インタフェースの統計情報を削除します。
- **interface-number** 引数を指定すると、このコマンドは指定された VLAN インタフェースの統計情報を削除します。

例

VLAN インタフェース 2 の統計情報を削除します。

<AP> reset counters interface vlan-interface 2

関連コマンド

display interface vlan-interface

2.1.8 shutdown

Syntax

shutdown

undo shutdown

デフォルト

VLAN インタフェースは手動でシャットダウンしていません。以下のガイドラインが適用されます。

- VLAN のすべてのポートが down している場合、VLAN インタフェースは down になります。
- 1 つ以上の VLAN が up である場合、VLAN インタフェースは up になります。

View

VLAN interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドは VLAN インタフェースをシャットダウンします。

undo shutdown コマンドは VLAN インタフェースを up にします。

コマンドを使用した場合、VLAN インタフェースは DOWN（Administratively）状態のままになります。この場合、VLAN インタフェースの状態は VLAN のポートの状態に影響しません。

⚠ **注意:**

VLAN インタフェースで **shutdown** コマンドを実行すると、VLAN インタフェースのリンクが切断され、通信が中断されます。このコマンドは慎重に使用してください。

VLAN インタフェースのパラメータを設定する前に、ネットワークへの影響から設定を防ぐため、**shutdown** コマンドで VLAN インタフェースをシャットダウンしてください。VLAN インタフェースのパラメータを設定した後、設定を適用するため、**undo shutdown** コマンドを使用してください。

故障した VLAN インタフェースのトラブルシューティングを行うため、**shutdown** コマンドを使用してください。インタフェースが回復したかどうかを確認するため、**undo shutdown** コマンドを使用してください。

VLAN 内のすべての Ethernet ポートの状態は、VLAN インタフェースの状態とは無関係です。

例

VLAN インタフェース 2 をシャットダウンし、up にします。

<AP> system-view

[AP] interface vlan-interface 2

[AP-Vlan-interface2] shutdown

[AP-Vlan-interface2] undo shutdown

2.1.9 vlan

Syntax

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

デフォルト

VLAN 1（システムデフォルト VLAN）

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id1,vlan-id2: VLAN ID を指定します。設定範囲は 1～4094 です。

vlan-id1 **to** *vlan-id2*: VLAN の範囲を指定します。*vlan-id1* と *vlan-id2* は VLAN ID を指定します。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: VLAN 1～4094 を指定します。

説明

vlan *vlan-id* コマンドは VLAN を作成し、その view あるいは既存の VLAN の view に移行します。

vlan *vlan-id1* **to** *vlan-id2* コマンドは *vlan-id1* から *vlan-id2* の VLAN を作成します。

vlan all コマンドは VLAN 1～VLAN 4094 を作成します。

undo vlan コマンドは指定された VLAN を削除します。

システムデフォルト VLAN（VLAN 1）を作成あるいは削除することはできません。

ダイナミック VLAN、アプリケーションによって固定された VLAN を削除するため、**undo vlan** コマンドを使用することはできません。これらの VLAN を削除するため、最初に VLAN から設定を削除してください。

例

VLAN 2 を作成し、その view に移行します。

<AP> system-view

[AP] vlan 2

[AP-vlan2]

VLAN 4～VLAN 100 を作成します。

<AP> system-view

[AP] vlan 4 to 100

関連コマンド

display vlan

2.2 ポートベースVLAN設定コマンド

2.2.1 display port

Syntax

display port { **hybrid** | **trunk** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

hybrid: ハイブリッドポートを指定します。

trunk: トランクポートを指定します。

説明

display port コマンドはハイブリッドポートあるいはトランクポートに関する情報を表示します。

例

ハイブリッドポートの情報を表示します。

<AP> display port hybrid

```
Interface            PVID  VLAN Passing
GE1/0/1              100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                                    2555-2558, 3000, 4000
                           Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                                    150-160, 200, 255, 286, 300-302
```

トランクポートの情報を表示します。

<AP> display port trunk

```
Interface            PVID  VLAN Passing
GE1/0/1              2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                           555, 600-611, 1000, 2006-2008
```

表 2-5 コマンド出力

フィールド	説明
Interface	ポート名です。

フィールド	説明
PVID	ポートのVLAN IDです。
VLAN Passing	ポートで許可されたVLANです。
Tagged	VLANタグを削除しないでポートがパケットを送信するVLANです。
Untagged	VLANタグを削除した後、ポートがパケットを送信するVLANです。

2.2.2 port

Syntax

port *interface-list*

undo port *interface-list*

デフォルト

VLAN 1

View

VLAN view

定義済みユーザロール

network-admin

パラメータ

interface-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number1* [**to** *interface-type interface-number2*]です。*interface-number2* は *interface-number1* 以上の値にしてください。

説明

port コマンドは指定したアクセスポートに VLAN を割り当てます。

undo port コマンドは VLAN から指定したアクセスポートを削除します。

このコマンドはアクセスポートのみ適用可能です。

デフォルトですべてのポートはアクセスポートです。ポートタイプを **port link-type** コマンドで設定することができます。

例

GigabitEthernet 1/0/1 に VLAN 2 を割り当てます。

<AP> system-view

[AP] vlan 2

[AP-vlan2] port gigabitethernet 1/0/1

関連コマンド

display vlan

2.2.3 port access vlan

Syntax

port access vlan *vlan-id*

undo port access vlan

デフォルト

すべての VLAN は VLAN1 に所属しています。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port access vlan コマンドはアクセスポートを指定した VLAN に割り当てます。

undo port access vlan コマンドはデフォルトに戻します。

アクセスポートを VLAN に割り当てる前に、VLAN が作成されていることを確認してください。

例

GigabitEthernet 1/0/1 に VLAN 3 を割り当てます。

<AP> system-view

[AP] vlan 3

[AP-vlan3] quit

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] port access vlan 3

2.2.4 port hybrid pvid

Syntax

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートの PVID はポートが所属している VLAN の ID です。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port hybrid pvid コマンドはハイブリッドポートの PVID を設定します。

undo port hybrid pvid コマンドはハイブリッドポートの PVID を 1 に設定します。

ハイブリッドポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドでハイブリッドポートの PVID を削除する場合、ポートの PVID の設定は適用されません。

ローカルとリモートのハイブリッドポートに同じ PVID を設定することを推奨します。

PVID からのパケットの転送を許可するためにハイブリッドポートの設定に **port hybrid pvid** コマンドを使用してください。

例

ハイブリッドポートの GigabitEthernet 1/0/1 の PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 をタグなしメンバとして割り当てます。

<AP> system-view

[AP] vlan 100

[AP-vlan100] quit

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] port link-type hybrid

[AP-GigabitEthernet1/0/1] port hybrid pvid vlan 100

[AP-GigabitEthernet1/0/1] port hybrid vlan 100 untagged

関連コマンド

- **port hybrid vlan**
- **port link-type**

2.2.5 port hybrid vlan

Syntax

port hybrid vlan *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

デフォルト

リンクタイプがアクセスであるとき、ハイブリッドポートはポートが所属している VLAN のタグなしメンバです。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

tagged: ポートは VLAN タグを削除しないで指定した VLAN のパケットを送信するように設定します。

untagged: ポートは VLAN タグを削除したのち、指定した VLAN のパケットを送信するように設定します。

説明

port hybrid vlan コマンドは指定した VLAN にハイブリッドポートを割り当てます。

undo port hybrid vlan コマンドは指定した VLAN からハイブリッドポートを削除します。

ハイブリッドポートは、複数の VLAN が通過できます。**port hybrid vlan** コマンドを繰り返し実行すると、ハイブリッドポートを通過する VLAN は、各実行の *vlan-id-list* により指定された VLAN に設定されます。

例

GigabitEthernet 1/0/1 をハイブリッドポートに設定します。VLAN 2、VLAN 4 および VLAN 50～VLAN 100 に割り当て、これらの VLAN のパケットにタグを付けて送信するよう GigabitEthernet 1/0/1 に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] port link-type hybrid

[AP-GigabitEthernet1/0/1] port hybrid vlan 2 4 50 to 100 tagged

関連コマンド

port link-type

2.2.6 port link-type

Syntax

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

デフォルト

access

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

access: ポートのリンクタイプをアクセスとして指定します。

hybrid: ポートのリンクタイプをハイブリッドとして指定します。

trunk: ポートのリンクタイプをトランクとして指定します。

説明

port link-type コマンドはポートのリンクタイプを設定します。

undo port link-type コマンドはデフォルトに戻します。

トランクポートからハイブリッドポート（またはその逆）のリンクタイプを変更するには、まずリンクタイプをアクセスに設定する必要があります。

例

GigabitEthernet 1/0/1 のリンクタイプをトランクポートに設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] port link-type trunk

2.2.7 port trunk permit vlan

Syntax

port trunk permit vlan { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

デフォルト

トランクポートは VLAN 1 からのパケットのみ通過できるように許可します。

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、VLAN ID の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* **to** *vlan-id2* です。設定範囲は 1〜4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: すべての VLAN を通過できるように許可します。許可されていない VLAN ユーザがポートを通して制限されたリソースにアクセスすることを防ぐため、注意して **port trunk permit vlan all** コマンドを使用してください。

説明

port trunk permit vlan コマンドはトランクポートを指定した VLAN に割り当てます。

undo port trunk permit vlan コマンドはトランクポートを指定した VLAN から削除します。

トランクポートは複数の VLAN を通過できます。**port trunk permit vlan** コマンドを繰り返し実行すると、トランクポートを通過する VLAN は、各 *vlan-id-list* により指定された VLAN に設定されます。

トランクポート上では、PVID のトラフィックのみタグなしで通過することができます。

例

GigabitEthernet 1/0/1 をトランクポートに設定します。VLAN 2、VLAN 4 および VLAN 50〜VLAN 100 に割り当てます。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] port link-type trunk

[AP-GigabitEthernet1/0/1] port trunk permit vlan 2 4 50 to 100

関連コマンド

port link-type

2.2.8 port trunk pvid

Syntax

port trunk pvid vlan *vlan-id*

undo port trunk pvid

デフォルト

VLAN 1

View

Layer 2 aggregate interface view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN ID を指定します。設定範囲は 1～4094 です。

説明

port trunk pvid コマンドはトランクポートの PVID を設定します。

undo port trunk pvid コマンドはデフォルトに戻します。

トランクポートの PVID として存在しない VLAN を使用することができます。**undo vlan** コマンドを使用してトランクポートの PVID を削除しても、ポートの PVID の設定には影響しません。

ローカルおよびリモートのトランクポートは、PVID のトラフィックが正常に送信されるために同じ PVID を使用する必要があります。

PVID からのパケットの転送を許可するためにトランクポートの設定に **port trunk permit vlan** コマンドを使用してください。

例

GigabitEthernet 1/0/1 をトランクポートに設定します。PVID を VLAN 100 に設定し、GigabitEthernet 1/0/1 に VLAN 100 を割り当てます。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] port link-type trunk

[AP-GigabitEthernet1/0/1] port trunk pvid vlan 100

[AP-GigabitEthernet1/0/1] port trunk permit vlan 100

関連コマンド

- **port link-type**
- **port trunk permit vlan**

目次

このセクションのページは **4-x-x** です。

3 章 ループ検出 3-1
3.1 ループ検出設定コマンド 3-1
3.1.1 display loopback-detection 3-1
3.1.2 loopback-detection action 3-3
3.1.3 loopback-detection enable 3-5
3.1.4 loopback-detection global action 3-6
3.1.5 loopback-detection global enable 3-7
3.1.6 loopback-detection interval-time 3-8

3章 ループ検出

3.1 ループ検出設定コマンド

3.1.1 display loopback-detection

Syntax

display loopback-detection

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display loopback-detection コマンドはループバック検出の設定と状態を表示します。

例

ループバック検出の設定と状態を表示します。

<AP> display loopback-detection

```
Loopback detection is enabled.
Loopback detection interval is 30 second(s).
Loopback is detected on following interfaces:
 Interface             Action mode
 GigabitEthernet1/0/1    Block
 GigabitEthernet1/0/2    Shutdown
 GigabitEthernet1/0/3    None
 GigabitEthernet1/0/4    No-learning
```

表 3-1 コマンド出力

フィールド	説明
Action mode	ループガードのアクションです。 • **Block**–ポートでループが検出されたとき、装置は以下の処理を行います。 　• ログを出力します。 　• MACアドレスの学習を無効にします。 　• ポート上の着信トラフィックをブロックします。 • **None**–ポートでループが検出されたとき、装置はログを出力しますが、ポートでアクションは行いません。 • **No-learning**–ポートでループが検出されたとき、装置はログを出力し、MACアドレスの学習を無効にします。 🕮 **メモ：** **loopback-detection action shutdown**コマンドを設定し、ポートでループが検出されたとき、ポートがシャットダウンします。ポートのシャットダウンによってループ状態が解除されるため、**display loopback-detection**コマンド上に検知ポートは表示されません。“Shutdown”状態が表示されることはありません。
VLANs	ループが検出されたVLANです。

3.1.2 loopback-detection action

Syntax

loopback-detection action { **block** | **no-learning** | **shutdown** }

undo loopback-detection action

デフォルト

ポートでループが検出されたとき、装置はログを出力しますが、ポートでアクションは行いません。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

block: ブロックモードを有効にします。ループを検出すると、装置は以下の処理を行います。

- ログを出力します。
- MAC アドレスの学習を無効にします。
- ポートの入力トラフィックをブロックします。

no-learning: **no-learning** モードを有効にします。ループを検出すると、装置はログを出力し、MAC アドレスの学習を無効にします。アグリゲートインタフェースではサポートしていません。

shutdown: シャットダウンモードを有効にします。ループを検出すると、装置はログを出力し、すべてのフレームの送受信を無効にするためポートをシャットダウンします。装置は検出タイマが終了すると、自動でポートをアップします。**shutdown-interval** コマンドで検出タイマを設定することができます。詳細はコマンドマニュアルのセクション 2 *システム管理　“装置管理”* を参照してください。

説明

loopback-detection action コマンドはポートのループ保護のアクションを設定します。

undo loopback-detection action コマンドはデフォルトに戻します。

グローバルでループ保護のアクションを設定する場合、**loopback-detection global action** コマンドを使用します。

グローバルの設定はすべてのポートで適用されます。ポートの設定は指定されたポートで適用されます。ポートの設定はグローバルの設定よりも優先されます。

例

GigabitEthernet 1/0/1 のループ保護のアクションをシャットダウンに設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] loopback-detection action shutdown

関連コマンド

- **display loopback-detection**
- **loopback-detection global action**

3.1.3 loopback-detection enable

Syntax

loopback-detection enable vlan { *vlan-id-list* | **all** }

undo loopback-detection enable vlan { *vlan-id-list* | **all** }

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN リストを指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: 既存のすべての VLAN を指定します。

説明

loopback-detection enable コマンドはポートでループ検出を有効にします。

undo loopback-detection enable コマンドはポートでループ検出を無効にします。

グローバルでループ検出を有効にする場合、**loopback-detection global enable** コマンドを使用します。

ポートのループ検出の設定はグローバルでループ検出の設定が行われたのち適用されます。

グローバル設定は、指定された VLAN のすべてのポートに適用されます。ポート単位の設定は、ポートが指定された VLAN に属する場合にのみ、個々のポートに適用されます。ポート単位の設定は、グローバル設定よりも優先されます。

例

VLAN 10～VLAN 20 の GigabitEthernet 1/0/1 でループ検出を有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] loopback-detection enable vlan 10 to 20

関連コマンド

- **display loopback-detection**

- **loopback-detection global enable**

3.1.4 loopback-detection global action

Syntax

loopback-detection global action shutdown

undo loopback-detection global action

デフォルト

ループが検出されたとき、装置はログを出力しますが、保護アクションは行いません。

View

System view

定義済みユーザロール

network-admin

パラメータ

shutdown: シャットダウンモードを有効にします。ループを検出すると、装置はログを出力し、ポートをシャットダウンします。装置は検出タイマが終了すると、自動でポートを転送状態にします。**shutdown-interval** コマンドで検出タイマを設定することができます。詳細はコマンドマニュアルのセクション 1 *基本機能 “装置管理”* を参照してください。

説明

loopback-detection global action コマンドはグローバルでループ保護のアクションを設定します。

undo loopback-detection global action コマンドはデフォルトに戻します。

ポートでループ保護のアクションを設定する場合、interface view で **loopback-detection action** コマンドを使用します。

グローバルの設定はすべてのポートで適用されます。ポートの設定は指定されたポートで適用されます。ポートの設定はグローバルの設定よりも優先されます。

🕮 **メモ：**

- **shutdown** アクションを設定し、ポートでループが検出されたとき、ポートをシャットダウンし、ループ状態を解除するため、アクション実行時に RECOVERED のログも出力します。
- **shutdown** アクションによるポートのシャットダウンは、**display interface** コマンドの Current state フィールドの状態が DOWN（Loopback detection down）と表示されます。

例

グローバルでループ保護のアクションをシャットダウンに設定します。

<AP> system-view

[AP] loopback-detection global action shutdown

関連コマンド

- **display loopback-detection**
- **loopback-detection action**

3.1.5 loopback-detection global enable

Syntax

loopback-detection global enable vlan { *vlan-id-list* | **all** }

undo loopback-detection global enable vlan { *vlan-id-list* | **all** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN リストを指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。設定範囲は 1～4094 です。*vlan-id2* は *vlan-id1* 以上の値にしてください。

all: 既存のすべての VLAN を指定します。

説明

loopback-detection global enable コマンドはグローバルでループ検出を有効にします。

undo loopback-detection global enable コマンドはグローバルでループ検出を無効にします。

ポートでループ検出を有効にする場合、interface view で **loopback-detection enable** コマンドを使用します。

グローバルの設定は指定された VLAN のすべてのポートで適用されます。ポートの設定は指定された VLAN に所属するポートで適用されます。ポート単位の設定は、ポートが指定された VLAN に属する場合にのみ、個々のポートに適用されます。ポートの設定はグローバルの設定よりも優先されます。

例

VLAN 10～VLAN 20 のすべてのポートでループ検出を有効にします。

<AP> system-view

[AP] loopback-detection global enable vlan 10 to 20

関連コマンド

- **display loopback-detection**
- **loopback-detection enable**

3.1.6 loopback-detection interval-time

Syntax

loopback-detection interval-time *interval*

undo loopback-detection interval-time

デフォルト

5 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: ループ検出間隔を設定します。設定範囲は 1～300 秒です。

説明

loopback-detection interval-time コマンドはループ検出間隔を設定します。

undo loopback-detection interval-time コマンドはデフォルトに戻します。

ループ検出が有効であるとき、装置は指定された間隔でループ検出フレームを送信します。検出間隔が短い場合、精度が高くなりますが、多くのリソースが消費されます。ループ検出間隔を設定する場合、システムの性能とループ検出速度を考慮してください。

🕮 **メモ：**

undo loopback-detection interval-time コマンドを実行しても、デフォルト設定には戻りません。**undo** コマンドを実行した場合は、30 秒のループ検出間隔で動作する設定となります。デフォルト値に戻す場合は、**loopback-detection interval-time 5** コマンドを実行してください。

例

ループ検出間隔を 10 秒に設定します。

<AP> system-view

[AP] loopback-detection interval-time 10

関連コマンド

display loopback-detection

目次

このセクションのページは **4-x-x** です。

4 章 スパニングツリー 4-1
4.1 スパニングツリー設定コマンド 4-1
4.1.1 active region-configuration 4-1
4.1.2 check region-configuration 4-2
4.1.3 display stp 4-4
4.1.4 display stp abnormal-port 4-10
4.1.5 display stp bpdu-statistics 4-12
4.1.6 display stp down-port 4-15
4.1.7 display stp history 4-16
4.1.8 display stp region-configuration 4-17
4.1.9 display stp root 4-20
4.1.10 display stp tc 4-21
4.1.11 instance 4-22
4.1.12 region-name 4-24
4.1.13 reset stp 4-25
4.1.14 revision-level 4-26
4.1.15 stp bpdu-protection 4-27
4.1.16 stp bridge-diameter 4-28
4.1.17 stp compliance 4-29
4.1.18 stp config-digest-snooping 4-30
4.1.19 stp cost 4-31
4.1.20 stp edged-port 4-33
4.1.21 stp enable 4-35
4.1.22 stp global config-digest-snooping 4-36
4.1.23 stp global enable 4-37
4.1.24 stp global mcheck 4-38
4.1.25 stp loop-protection 4-38
4.1.26 stp max-hops 4-40
4.1.27 stp mcheck 4-41
4.1.28 stp mode 4-43
4.1.29 stp no-agreement-check 4-44
4.1.30 stp pathcost-standard 4-45
4.1.31 stp point-to-point 4-46
4.1.32 stp port priority 4-48
4.1.33 stp priority 4-49
4.1.34 stp pvst-bpdu-protection 4-50

4.1.35 stp region-configuration 4-51
4.1.36 stp root primary 4-51
4.1.37 stp root secondary 4-53
4.1.38 stp root-protection 4-54
4.1.39 stp tc-protection 4-55
4.1.40 stp tc-protection threshold 4-56
4.1.41 stp timer forward-delay 4-56
4.1.42 stp timer hello 4-58
4.1.43 stp timer max-age 4-59
4.1.44 stp timer-factor 4-60
4.1.45 stp transmit-limit 4-62
4.1.46 vlan-mapping modulo 4-64

4章 スパニングツリー

4.1 スパニングツリー設定コマンド

4.1.1 active region-configuration

Syntax

active region-configuration

View

MST region view

定義済みユーザロール

network-admin

説明

active region-configuration コマンドは MST(multiple spanning tree)リージョン設定をアクティブにします。

MST リージョンパラメータを設定するとき、MSTP は新しいスパニングツリーの計算プロセスを行います。スパニングツリーの計算プロセスが実行されるとネットワークが不安定になります。VLAN-インスタンスマッピングテーブルを設定するときに、よく発生します。このため **active region-configuration** コマンドあるいは **stp global enable** コマンドを実行したのち、MSTP を有効にします。

このコマンドを実行する前に、**check region-configuration** コマンドを使用して MST のリージョンの設定が正しいことを確認してください。MST のリージョンの設定が正しいことが確認できたら、このコマンドを実行してください。

例

MSTI 1 に VLAN 2 をマッピングし、MST リージョンの設定を有効にします。

<AP> system-view

[AP] stp region-configuration

[AP-mst-region] instance 1 vlan 2

[AP-mst-region] active region-configuration

関連コマンド

- **check region-configuration**
- **instance**
- **region-name**
- **revision-level**

- **stp global enable**

4.1.2 check region-configuration

Syntax

check region-configuration

View

MST region view

定義済みユーザロール

network-admin

説明

check region-configuration コマンドはリージョン名、リビジョンレベル、VLAN-インスタンスマッピング設定などの、まだアクティブにされていない MST リージョンの設定の情報を表示します。

スパニングツリーの装置は物理リンクを通して接続され、以下の設定が同一であるときのみ、同じ MST リージョンに属します。

- フォーマットセレクタ（デフォルトは 0 で設定できません。）
- MST リージョン名
- MST リージョンリビジョンレベル
- MST リージョンの VLAN-インスタンスマッピングエントリ

MST リージョンの設定をアクティブにする前に、MST のリージョン設定が正しいかどうかをチェックするために、このコマンドを使うことを推奨します。結果が正しいときのみ、MST リージョン設定をアクティブにしてください。

例

MST リージョンのまだアクティブにされていない設定の情報を表示します。

<AP> system-view

[AP] stp region-configuration

[AP-mst-region] check region-configuration

```
Admin Configuration
  Format selector      : 0
  Region name          : 001122334400
  Revision level       : 0
  Configuration digest : 0x3ab68794d602fdf43b21c0b37ac3bca8

  Instance  VLANs Mapped
  0         1, 3 to 4094
```

```
15        2
```

表 4-1 コマンド出力

フィールド	説明
Format selector	フォーマットセレクタです。値は0です（設定はできません）
Region name	MST リージョン名です。
Revision level	MSTリージョンのリビジョンレベルです。
Instance VLANs Mapped	MSTリージョンのVLAN-インスタンスマッピングエントリです。

関連コマンド

- **active region-configuration**
- **instance**
- **region-name**
- **revision-level**

4.1.3 display stp

Syntax

display stp [**instance** *instance-list*] [**interface** *interface-list*] [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

interface *interface-list*: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number 1* [**to** *interface-type interface-number 2*]です。*interface-number 2* は *interface-number 1* 以上の値にしてください。

brief: スパニングツリーの状態と統計情報の概要を表示します。指定しない場合、詳細なスパニングツリーの状態と統計情報を表示します。

説明

display stp コマンドはスパニングツリーの状態と統計情報を表示します。スパニングツリーの状態および統計情報にもとづいて、ネットワークトポロジの分析および維持、あるいはスパニングツリーが正常に動作しているか確認することができます。

STP あるいは RSTP モード：コマンド出力はポート名の順番で表示されます。

- ポートを指定しない場合、すべてのポートに適用されます。
- ポートリストを指定した場合、指定したポートに適用されます。

MSTP モード：コマンド出力はそれぞれの MSTI の MSTI ID とポート名の順番で表示されます。

- MSTI あるいはポートを指定しない場合、すべてのポートの MSTI に適用されます。
- MSTI を指定し、ポートを指定しない場合、指定した MSTI のすべてのポートに適用されます。
- MSTI およびポートリストを指定した場合、指定した MSTI の指定ポートに適用されます。
- MSTI リストとポートリストの両方を指定した場合、このコマンドは指定した MSTI の指定したポートに適用されます。

ネットワークの収束中、最新のスパニングツリーの情報は表示されません。

例

MSTP モードで、MSTI0 の GigabitEthernet 1/0/1 のスパニングツリーの状態と概要情報を表示します。

<AP> display stp instance 0 interface gigabitethernet 1/0/1 brief

```
MST ID     Port                      Role  STP State     Protection
 0         GigabitEthernet1/0/1        ALTE  DISCARDING    LOOP
```

表 4-2 コマンド出力

フィールド	説明
MST ID	MSTリージョンのMSTI IDです。
Port	各MSTIあるいはVLANに対応するポート名です。
Role	ポートの役割です。 • **ALTE**—代理ポートです。 • **BACK**—バックアップポートポートです。 • **ROOT**—ルートポートです。 • **DESI**—Designatedポートです。 • **MAST**—マスタポートです。 • **DISA**—ポートが無効です。
STP State	ポートのスパニングツリーの状態です。 • **FORWARDING**—ポートはBPDUを送受信し、ユーザトラフィックを転送します。 • **DISCARDING**—ポートはBPDUを送受信できますが、ユーザトラフィックを転送できません。 • **LEARNING**—ポートは過渡状態です。ポートはBPDUを送受信できますが、ユーザトラフィックを転送できません。
Protection	ポートの保護タイプです。 • **ROOT**—Rootガードです。 • **LOOP**—Loopガードです。 • **BPDU**—BPDUガードです。 • **NONE**—保護していません。

MSTP モードで、すべてのポートのすべての MSTI のスパニングツリーの状態と詳細情報を表示します。

<AP> display stp

```
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID          : 32768.0440-A900-0000
```

```
Bridge times       : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
Root ID/ERPC       : 32768.0440-A900-0000, 0
RegRoot ID/IRPC    : 32768.0440-A900-0000, 0
RootPort ID        : 0.0
BPDU-Protection    : Disabled
Bridge Config-
Digest-Snooping    : Disabled
TC or TCN received  : 2
Time since last TC  : 0 days 0h:0m:58s
. . .
```

MSTP モードで、スパニングツリー機能が無効であるときのスパニングツリーの状態と詳細情報を表示します。スパニングツリー機能がグローバルで有効でない場合、**STP is not configured** と表示されます。

<AP> display stp

```
Protocol status    : Disabled
Protocol Std.      : IEEE 802.1s
Version           : 3
Bridge-Prio.  : 32768
MAC address        : 0440-A900-0000
Max age(s)         : 20
Forward delay(s)   : 15
Hello time(s)      : 2
Max hops          : 20
TC Snooping        : Disabled
```

表 4-3 コマンド出力

フィールド	説明
Bridge ID	ブリッジのIDです。装置のプライオリティとMACアドレスを含みます。たとえば32768.000f-e200-2200において、ピリオド（.）の前の値は装置のプライオリティを示し、ピリオド（.）の後の値は装置のMACアドレスを示します。
Bridge times	ブリッジの主要パラメータです。 • **Hello**—Hello時間です。 • **MaxAge**—最大エージングタイマです。 • **FwdDelay**—転送遅延時間です。 • **MaxHops**—MSTリージョンの最大ホップ数です。
Root ID/ERPC	CISTルートIDと外部パスコストです。（装置からCISTルートまでのパスコストです）

フィールド	説明
RegRoot ID/IRPC	CISTリージョナルルートIDと内部パスコストです。（装置からCISTリージョナルルートまでのパスコストです）
RootPort ID	ルートポートIDです。0.0は装置がルートでルートポートがないことを示します。
BPDU-Protection	BPDU保護のグローバル状態を示します。
Bridge Config-Digest-Snooping	Digest Snoopingのグローバル状態を示します。
TC or TCN received	MSTIあるいはVLANで受信されたTC/TCNパケット数です。
Time since last TC	MSTIあるいはVLANで最後にトポロジが変更されてからの経過時間です。
Port protocol	ポートのスパニングツリーの状態です。
Port role	ポートの役割です。 • **Alternate**—代理ポートです。 • **Backup**—バックアップポートポートです。 • **Root**—ルートポートです。 • **Designated**—Designatedポートです。 • **Master**—マスタポートです。 • **Disabled**—ポートが無効です。
(Boundary)	ポートが境界ポートです。
Port cost(Legacy)	ポートのパスコストです。括弧の中身はポートパスコストの計算で使用される標準(**legacy**、**dot1d-1998**、あるいは **dot1t**)を示します。 • **Config**－設定値です。 • **Active**－実際の値です。
Desg.bridge/port	ポートのDesignated ブリッジIDとポートIDです。 表示されたポートIDは、ポートプライオリティをサポートしないポートであるため、重要ではありません。
Port edged	edgeポートあるいは非edgeポートです。 • **Config**－設定値です。 • **Active**－実際の値です。
Point-to-Point	ポートがポイントツーポイントで接続されているかどうかを示します。 • **Config**－設定値です。 • **Active**－実際の値です。
Transmit limit	各Hello時間以内に送信されたBPDU数です。

フィールド	説明
Protection type	ポートの保護タイプです。 ● **ROOT**—Rootガードです。 ● **LOOP**—Loopガードです。 ● **BPDU**—BPDUガードです。 ● **NONE**—保護していません。
TC-Restriction	ポートのTC転送の制限の状態です。 TC-Restrictionはサポートしていません。
Role-Restriction	ポートのポート役割の制限の状態です。
MST BPDU format	ポートが送信可能なMST BPDUの形式です。 ● **Config**－設定値（legacyあるいは802.1s準拠）です。 ● **Active**－実際の値（legacyあるいは802.1s準拠）です。
Port Config- Digest-Snooping	ポートのDigest Snoopingの状態です。
Rapid transition	MSTIあるいはVLANでポートの転送状態が高速状態遷移であるかどうかを示します。
Num of VLANs mapped	MSTIにマッピングされたVLAN数です。
Port times	ポートの主要パラメータです。 ● **Hello**—Hello時間です。 ● **MaxAge**—最大エージングタイマです。 ● **FwdDelay**—転送遅延時間です。 ● **MsgAge**—メッセージのエージングタイマ ● **RemHops**—残りのホップ数です。
BPDU sent	送信BPDUの統計情報です。
BPDU received	受信BPDUの統計情報です。
RegRoot ID/IRPC	MSTIリージョナルルートと内部パスのコストです。
Root Type	MSTIルートタイプです。 ● プライマリルートです。 ● セカンダリルートです。
Master bridge	MSTIルートブリッジIDです。
Cost to master	MSTIからマスタブリッジへのパスコストです。
TC received	受信TC BPDUの数です。
Protocol status	スパニングツリープロトコルの状態です。

フィールド	説明
Protocol Std.	スパニングツリープロトコルが標準です。
Version	スパニングツリープロトコルのバージョンです。
Bridge-Prio.	● MSTPモードで、CISTの装置のプライオリティです。
Max age(s)	BPDUのエージングタイマです。（単位は秒です。）
Forward delay(s)	ポートの状態遷移遅延です。（単位は秒です。）
Hello time(s)	BPDUを送信するルートブリッジの送信間隔です。
Max hops	MSTIの最大ホップ数です。
TC Snooping	TC snoopingの状態です。 ● 有効 ● 無効

関連コマンド

reset stp

4.1.4 display stp abnormal-port

Syntax

display stp abnormal-port

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp abnormal-port コマンドは STP 保護処理によってブロックされたポートに関する情報を表示します。

例

Version 7.2.11 を含む以降のソフトウェア：

MSTI モードで STP 保護処理によってブロックされたポートに関する情報を表示します。

<AP> display stp abnormal-port

```
MST ID     Blocked Port              Reason
 1         GigabitEthernet1/0/1       Root-Protected
```

表 4-4 コマンド出力

フィールド	説明
MST ID	ブロックされたポートのMSTIです。
Blocked Port	ブロックされたポートの名前です。
Block Reason	ポートがブロックされた理由です。 • **Root-Protected**—Rootガード機能です。 • **Loop-Protected**—Loopガード機能です。 • **Loopback-Protected**—自己ループの保護です。MSTIのポートが送信したBPDUを受信しました。 • **Disputed**—Disputeの保護です。ポートは非ブロックのDesignatedポートから低いプライオリティのBPDUを受信しました。 • **InconsistentPortType-Protected**—ポートタイプ不一致保護です。 • **InconsistentPvid-Protected**—PVID不一致保護です。

4.1.5 display stp bpdu-statistics

Syntax

display stp bpdu-statistics [**interface** *interface-type interface-number* [**instance** *instance-list*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

説明

display stp bpdu-statistics コマンドはポートの BPDU 統計情報を表示します。

MSTP モード：コマンド出力はポート名と MSTI ID の順番で表示されます。

- MSTI あるいはポートを指定しない場合、すべてのポートのすべての MSTI に適用されます。
- ポートを指定し、MSTI を指定しない場合、ポートのすべての MSTI に適用されます。
- MSTI およびポートを指定した場合、指定したポートの指定した MSTI に適用されます。

STP、RSTP モード：コマンド出力はポート名の順番で表示されます。

- ポートを指定しない場合、すべてのポートに適用されます。
- ポート名を指定した場合、ポートに適用されます。

例

MSTP モードで GigabitEthernet 1/0/1 のすべての MSTI の BPDU 統計情報を表示します。

<AP> display stp bpdu-statistics interface gigabitethernet 1/0/1

```
Port: GigabitEthernet1/0/1

Instance-Independent:

Type                    Count     Last Updated
```

```
--------------------------- ---------- -----------------
Invalid BPDUs               0
Looped-back BPDUs           0
Max-aged BPDUs              0
TCN sent                    0
TCN received                0
TCA sent                    0
TCA received                2          10:33:12 01/13/2011
Config sent                 0
Config received             0
RST sent                    0
RST received                0
MST sent                    4          10:33:11 01/13/2011
MST received                151        10:37:43 01/13/2011

Instance 0:
Type                       Count      Last Updated
--------------------------- ---------- -----------------
Timeout BPDUs               0
Max-hoped BPDUs             0
TC detected                 1          10:32:40 01/13/2011
TC sent                     3          10:33:11 01/13/2011
TC received                 0
```

表 4-5 コマンド出力

フィールド	説明
Port	ポート名です。
Instance-Independent	特定のMSTIに関係ない統計情報です。
Type	統計項目です。
Looped-back BPDUs	BPDUを送信したのち、同一ポートで受信したBPDUです。
Max-aged BPDUs	最大エージングを超過したBPDUです。
TCN sent	TCN BPDUの送信数です。
TCN received	TCN BPDUの受信数です。
TCA sent	TCA BPDUsの送信数です。
TCA received	TCA BPDUの受信数です。

フィールド	説明
Config sent	Configuration BPDUの送信数です。
Config received	Configuration BPDUの受信数です。
RST sent	Configuration BPDUの送信数です。
RST received	RSTP BPDUの受信数です。
MST sent	RSTP BPDUの受信数です。
MST received	MSTP BPDUの送信数です。
Instance	特定のMSTIの統計情報です。
Timeout BPDUs	タイムアウトしたBPDUです。
Max-hoped BPDUs	最大ホップ数が超過したBPDUです。
TC detected	TC BPDUの検出数です。
TC sent	TC BPDUの送信数です。
TC received	TC BPDUの受信数です。
PVID inconsistency BPDUs	このフィールドは、現在のソフトウェアバージョンではサポートされていません。受信ポートと矛盾するPVIDを持つ受信PVST BPDUの数です。

4.1.6 display stp down-port

Syntax

display stp down-port

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp down-port コマンドは STP 保護機能によってシャットダウンされたポートに関する情報を表示します。

例

STP 保護機能によってシャットダウンされたポートに関する情報を表示します。

<AP> display stp down-port

```
Down Port                      Reason
GigabitEthernet1/0/1           BPDU-Protected
```

表 4-6 コマンド出力

フィールド	説明
Down Port	STP保護機能によってシャットダウンされたポート名です。
Reason	ポートがシャットダウンされた理由です。**BPDU-Protected**はBPDUガード機能を示します。

4.1.7 display stp history

Syntax

display stp [**instance** *instance-list*] **history**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。

説明

display stp history コマンドはポートのロール計算の履歴情報を表示します。

STP あるいは RSTP モードではポートのロール計算の時間の順番で表示されます。

MSTP モード：コマンド出力は MSTI ID と各 MSTI のポートのロール計算の時間の順番で表示されます。

- MSTI を指定しない場合、すべての MSTI に適用されます。
- MSTI リストを指定した場合、指定した MSTI に適用されます。

例

MSTP モードで、MSTI 2 のポートのロール計算の履歴情報を表示します。

<AP> display stp instance 2 history

```
 --------------- STP slot 1 history trace ---------------
 -------------------  Instance 2   ----------------------
Port GigabitEthernet1/0/1
   Role change        : ROOT->DESI (Aged)
   Time               : 2009/02/08 00:22:56
   Port priority      : 0.0440-A900-0000 0 0.0440-A900-0000 128.1
   Designated priority : 0.0440-A900-0000 0 0.0440-A900-0000 128.1
  . . .
```

表 4-7 コマンド出力

フィールド	説明
Port	ポート名です。
Role change	ポートの役割変更です。（**Aged**は設定BPDUのタイムアウトによって変更が起きたことを示します）
Time	ポートのロール計算の時間です。
Port priority	ポートの現在の優先順位です。 ● STPモード、RSTPモード、およびMSTPモードのIST (MSTI 0) の場合、ポートの優先順位には、共通ルートブリッジID、共通ルートブリッジへのパスのコスト、リージョナルルートブリッジID、リージョナルルートブリッジへのパスのコスト、指定ブリッジID、指定ポートID、および指定ポートからメッセージを受信するポートのIDが含まれ、スペースで区切られます。 ● PVSTモードおよびMSTPモードのCSTの場合、ポートの優先順位には、リージョナルルートブリッジID、リージョナルルートブリッジへのパスのコスト、指定ブリッジID、指定ポートID、および指定ポートからメッセージを受信するポートのIDが含まれ、スペースで区切られます。
Designated priority	現在のポートが指定ポートとして報告する優先度情報です。 ● STPモード、RSTPモード、およびMSTPモードのIST (MSTI 0) の場合、ポートプライオリティには、共通ルートブリッジID、共通ルートブリッジへのパスのコスト、リージョナルルートブリッジID、リージョナルルートブリッジへのパスのコスト、デバイスブリッジID、指定ポートID、および現在のポートIDが含まれ、スペースで区切られます。 ● PVSTモードおよびMSTPモードのCSTの場合、ポートプライオリティには、リージョナルルートブリッジID、リージョナルルートブリッジへのパスのコスト、デバイスブリッジID、指定ポートID、および現在のポートIDが含まれ、スペースで区切られます。

4.1.8 display stp region-configuration

Syntax

display stp region-configuration

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp region-configuration コマンドは有効な MST リージョンの設定情報を表示します。以下の情報があります。

- リージョン名
- リビジョンレベル
- ユーザ定義の VLAN-インスタンスマッピング

例

MSTP モードで有効な MST リージョンの設定情報を表示します。

<AP> display stp region-configuration

```
Oper Configuration
  Format selector     : 0
  Region name         : hello
  Revision level      : 0
  Configuration digest : 0x5f762d9a46311effb7a488a3267fca9f

  Instance   VLANs Mapped
  0          21 to 4094
  1          1 to 10
  2          11 to 20
```

表 4-8 コマンド出力

フィールド	説明
Format selector	スパニングツリープロトコルで定義されたフォーマットセレクタです。デフォルト値は0です。セレクタは設定できません。
Region name	MSTリージョン名です。
Revision level	MSTリージョンのリビジョンレベルです。**revision-level**コマンドを使って設定できます。デフォルトは0です。
VLANs Mapped	MSTIにマッピングされたVLANです。

関連コマンド

- **instance**
- **region-name**
- **revision-level**

4.1.9 display stp root

Syntax

display stp root

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display stp root コマンドはスパニングツリーのルートブリッジ情報を表示します。

例

MSTP モードですべてのスパニングツリーのルートブリッジ情報を表示します。

<AP> display stp root

```
MST ID  Root Bridge ID       ExtPathCost IntPathCost Root Port
0       0.0440-A900-0000     200200      0           GigabitEthernet1/0/1
```

表 4-9 コマンド出力

フィールド	説明
ExtPathCost	外部パスコストです。装置は自動的にポートのデフォルトパスコストを計算します。あるいはポートのパスコストを設定するために**stp cost** コマンドを使用することができます。
IntPathCost	内部パスコストです。装置は自動的にポートのデフォルトパスコストを計算します。あるいはポートのパスコストを設定するために**stp cost** コマンドを使用することができます。
Root Port	ルートポート名です。（装置のポートがMSTIのルートポートである場合のみ表示されます）

4.1.10 display stp tc

Syntax

display stp [**instance** *instance-list*] **tc**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

説明

display stp tc コマンドはポートで送受信する TC/TCN BPDU の統計情報を表示します。

STP あるいは RSTP モードでは、出力はポート名の順番で表示されます。

MSTP モード：コマンド出力は MSTI ID と各 MSTI のポート名の順番で表示されます。

- MSTI を指定しない場合、すべての MSTI に適用されます。
- MSTI リストを指定した場合、指定した MSTI に適用されます。

例

MSTP モードで MSTI 0 のすべてのポートで送受信する TC/TCN BPDU の統計情報を表示します。

<AP> display stp instance 0 tc

```
-------------- STP slot 1 TC or TCN count -------------
MST ID     Port                          Receive     Send
0         GigabitEthernet1/0/1             6          4
```

表 4-10 コマンド出力

フィールド	説明
Port	ポート名です。
Receive	各ポートが受信したTC/TCN BPDUの数です。
Send	各ポートが送信したTC/TCN BPDUの数です。

4.1.11 instance

Syntax

instance *instance-id* **vlan** *vlan-id-list*

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

デフォルト

CIST

View

MST region view

定義済みユーザロール

network-admin

パラメータ

instance-list: MSTI ID を指定します。設定範囲は 0〜4094 です。0 は CIST を示します。コマンドの設定範囲は 1〜4094 です。

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1〜4094 です。

説明

注意:

以下の状況下でグローバル Digest Snooping を使用する場合、注意してください。
- VLAN-インスタンスマッピングを修正します。
- デフォルトの MST リージョンの設定に戻します。

もしローカル装置が隣接装置と異なる VLAN-インスタンスマッピングを持っている場合、ループあるいはトラフィックの中断が発生します。

instance コマンドは VLAN のリストを MSTI にマッピングします。

undo instance コマンドは指定した VLAN あるいはすべての VLAN を CIST（MSTI 0）に再マッピングします。

undo instance コマンドで VLAN を指定しない場合、指定された MSTI にマッピングされたすべての VLAN は CIST に再マッピングされます。

同一の VLAN を異なる MSTI にマッピングすることはできません。インスタンスにマッピングされている VLAN を新たなインスタンスにマッピングすると、古いマッピングは自動的に削除されます。

VLAN-インスタンスマッピングを最大 65 の MSTI にマッピングすることができます。

このコマンドを設定した後、VLAN-インスタンスマッピングをアクティブにするため、**active region-configuration** コマンドを実行します。

例

VLAN 2 を MSTI 1 にマッピングします。

<AP> system-view

[AP] stp region-configuration

[AP-mst-region] instance 1 vlan 2

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**

4.1.12 region-name

Syntax

region-name *name*

undo region-name

デフォルト

装置の MST リージョン名は MAC アドレスです。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

name: MST リージョン名を指定します。設定範囲は 1～32 です。

説明

region-name コマンドは MST リージョン名を設定します。

undo region-name コマンドはデフォルトに戻します。

装置の MST リージョンは、装置の MST リージョン名、VLAN-インスタンスマッピングテーブルおよび MSTP リビジョンレベルによって決まります。

このコマンドを設定した後、MST リージョン名をアクティブにするため、**active region-configuration** コマンドを実行します。

例

装置の MST リージョン名を hello に設定します。

<AP> system-view

[AP] stp region-configuration

[AP-mst-region] region-name hello

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **instance**
- **revision-level**

4.1.13 reset stp

Syntax

reset stp [**interface** *interface-list*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-list*: インタフェースを指定します。半角スペースで区切り 10 まで設定するか、インタフェースの範囲で設定することができます。インタフェースを範囲で指定する形式は *interface-type interface-number 1* [**to** *interface-type interface-number 2*]です。*interface-number 2* は *interface-number 1* 以上の値にしてください。指定しない場合すべてのポートのスパニングツリーに関する統計情報を削除します。

説明

reset stp コマンドはスパニングツリーの統計情報を削除します。スパニングツリーの統計情報は、TCN BPDU の数、configuration BPDU、RST BPDU、および指定したポートで送受信された MST BPDU が含まれます。

例

GigabitEthernet 1/0/1 のスパニングツリーの統計情報を削除します。

<AP> reset stp interface gigabitethernet 1/0/1

関連コマンド

display stp

4.1.14 revision-level

Syntax

revision-level *level*

undo revision-level

デフォルト

0

View

MST region view

定義済みユーザロール

network-admin

パラメータ

level: MSTP リビジョンレベルを指定します。設定範囲は 0～65535 です。

説明

revision-level コマンドは MSTP リビジョンレベルを設定します。

undo revision-level コマンドはデフォルトに戻します。

装置の MSTP リビジョンレベル、MST リージョン名、VLAN-インスタンスマッピングテーブルは、装置の MST リージョンによって決まります。

このコマンドを設定した後、MST リージョン名をアクティブにするため、**active region-configuration** コマンドを実行します。

例

MST リージョンの MSTP リビジョンレベルを 5 に設定します。

<AP> system-view

[AP] stp region-configuration

[AP-mst-region] revision-level 5

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **instance**
- **region-name**

4.1.15 stp bpdu-protection

Syntax

stp bpdu-protection

undo stp bpdu-protection

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp bpdu-protection コマンドは BPDU ガード機能を有効にします。

undo stp bpdu-protection コマンドは BPDU ガード機能を無効にします。

BPDU ガードを有効にすると、デバイスはエッジポートをシャットダウンし、エッジポートが設定 BPDU を受信したときにシャットダウンイベントを NMS に通知します。

ポートステータス検出タイマの期限が切れると、デバイスはシャットダウンされたポートを再アクティブ化します。このタイマは、**shutdown-interval** コマンドを使用して設定できます。このコマンドの詳細については、 コマンドマニュアルセクション *2 システム管理の "装置管理"* を参照してください。

stp bpdu-protection コマンドは、**stp edged-port** コマンドを使用して設定されたエッジポートでのみ有効です。

例

BPDU ガード機能を有効にします。

<AP> system-view

[AP] stp bpdu-protection

関連コマンド

- **shutdown-interval**（セクション *2 システム管理の "装置管理"*）
- **stp edged-port**

4.1.16 stp bridge-diameter

Syntax

stp bridge-diameter *diameter*

undo stp bridge-diameter

デフォルト

7

View

System view

定義済みユーザロール

network-admin

パラメータ

diameter: スイッチネットワークのダイアメータを指定します。設定範囲は 2～7 です。

説明

stp bridge-diameter コマンドはスイッチネットワークのネットワークダイアメータを設定します。

undo stp bridge-diameter コマンドはデフォルトに戻します。

ネットワークダイアメータは、端末装置がルートブリッジを経由して、スイッチネットワーク上の別の端末装置に到達するためのステーションの最大数を示します。

Hello 時間、転送遅延、最大エージングタイマを適切に設定するとネットワーク収束の速度を上げることができます。これらのタイマの値はネットワークサイズに関連しています。ネットワークダイアメータを設定することで、これら 3 つのタイマを間接的に設定することができます。ネットワークダイアメータが 7（デフォルト値）に設定されていると、3 つのタイマもデフォルトに設定されます。

STP、RSTP、MSTP モードでは、各 MST リージョンは装置と認識され、CIST（あるいは共通ルートブリッジ）のみ適用することができます。

例

MSTP モードでスイッチネットワークのネットワークダイアメータを 5 に設定します。

<AP> system-view

[AP] stp bridge-diameter 5

関連コマンド

- **stp timer forward-delay**
- **stp timer hello**
- **stp timer max-age**

4.1.17 stp compliance

Syntax

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

デフォルト

auto

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

auto: ポートが自動で MSTP BPDU フォーマットを認識し、それに従って送信する MSTP BPDU のフォーマットを決定するよう設定します。

dot1s: ポートが標準フォーマット（802.1s 準拠）の MSTP BPDU のみ送受信するよう設定します。

legacy: ポートが互換性のあるフォーマットの MSTP BPDU のみを送受信するよう設定します。

説明

stp compliance コマンドは指定したポートが MSTP BPDU の認識および送信に使用するモードを設定します。

undo stp compliance コマンドはデフォルトに戻します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 が標準フォーマット（802.1s）の MSTP パケットのみを送信するよう設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp compliance dot1s

4.1.18 stp config-digest-snooping

Syntax

stp config-digest-snooping

undo stp config-digest-snooping

デフォルト

無効

View

Layer 2 Ethernet interface view,

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp config-digest-snooping コマンドは Digest Snooping を有効にします。

undo stp config-digest-snooping コマンドは Digest Snooping を無効にします。

この設定はグローバル、およびほかのベンダの装置に接続されたポートの両方で有効にする必要があります。影響を最小限にするため、グローバルで有効にする前に関連したポートの機能を有効にしてください。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

Digest Snooping を GigabitEthernet 1/0/1 とグローバルで有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp config-digest-snooping

[AP-GigabitEthernet1/0/1] quit

[AP] stp global config-digest-snooping

関連コマンド

- **display stp**
- **stp global config-digest-snooping**

4.1.19 stp cost

Syntax

stp [**instance** *instance-list*] **cost** *cost-value*

undo stp [**instance** *instance-list*] **cost**

デフォルト

装置は各スパニングツリーのポートのパスコストを、対応する標準にもとづいて自動的に計算します。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

cost-value: 使用するパスコスト計算標準によって異なる有効範囲で、ポートのパスコストを指定します。。

- パスコスト計算に IEEE 802.1d-1998 が選択されている場合、設定範囲は 1～65535 です。
- パスコスト計算に IEEE 802.1t が選択されている場合、設定範囲は 1～200000000 です。
- パスコスト計算にプライベート標準が選択されている場合、コスト範囲は 1～200000 です。

説明

stp cost コマンドはポートのパスコストを設定します。

undo stp cost コマンドはデフォルトに戻します。

パスコストはスパニングツリー計算を行う際の重要な要素です。MSTI のポートに異なるパスコストを設定すると、VLAN トラフィックのフローが異なる物理的リンクを通って転送され、VLAN ベースのロードバランスを行うことができます

ポートのパスコストの設定はポートの役割に影響します。ポートの役割が変更されたとき、システムはポートの役割を計算し、状態遷移を開始します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

MSTI あるいは VLAN を指定しない場合、このコマンドは MSTP CIST あるいは STP、RSTP スパニングツリーのポートのパスコストを設定します。

例

MSTP モードで MSTI 2 の GigabitEthernet 1/0/1 のパスコストを 200 に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp instance 2 cost 200

関連コマンド

- **display stp**
- **stp pathcost-standard**

4.1.20 stp edged-port

Syntax

stp edged-port

undo stp edged-port

デフォルト

すべてのポートは非エッジポートです。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp edged-port コマンドはポートを Edge ポートに設定します。

undo stp edged-port コマンドはポートを非 Edge ポートに設定します。

ユーザ端末に直接接続しているポートは別の装置あるいは共有 LAN セグメントに接続されているポートよりも、Edge ポートとして設定されることができます。

ネットワークトポロジが変化した場合、Edge ポートは一時ループを起こしません。

ポートを Edge ポートとして設定すると、そのポートは早急に転送状態に遷移することができます。ユーザ端末に直接接続されているポートを Edge ポートとして設定することを推奨します。

通常､Edge ポートはほかの装置に接続されていないため､ほかの装置からの configuration BPDU は、Edge ポートには到達しません。BPDU ガード機能が無効であるとき、configuration BPDU を受信すると、Edge ポートとして設定されたポートは非 Edge ポートとして動作します。

ポートでループガード機能と Edge ポートの設定は同時に設定することはできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 を Edge ポートとして設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp edged-port

関連コマンド

- **stp bpdu-protection**
- **stp loop-protection**
- **stp root-protection**

4.1.21 stp enable

Syntax

stp enable

undo stp enable

デフォルト

有効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp enable コマンドはスパニングツリー機能を有効にします。

undo stp enable コマンドはスパニングツリー機能を無効にします。

スパニングツリー機能を有効にしたとき、装置はスパニングツリーのモードの設定に従い STP、RSTP、MSTP モードで動作します。

スパニングツリー機能を有効にしたとき、装置は受信した configuration BPDU にもとづいて VLAN のスパニングツリーの状態を自動で維持します。

スパニングツリー機能を無効にしたとき、装置はスパニングツリーの状態の維持を停止します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

MSTP モードで、GigabitEthernet 1/0/1 のスパニングツリー機能を無効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] undo stp enable

関連コマンド

- **stp global enable**
- **stp mode**

4.1.22 stp global config-digest-snooping

Syntax

stp global config-digest-snooping

undo stp global config-digest-snooping

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp global config-digest-snooping コマンドはグローバルで Digest Snooping を有効にします。

undo stp global config-digest-snooping コマンドはグローバルで Digest Snooping を無効にします。

この設定はグローバル、およびほかのベンダの装置に接続されたポートの両方で有効にする必要があります。影響を最小限にするため、グローバルで有効にする前に関連したポートの機能を有効にしてください。

例

Digest Snooping を GigabitEthernet 1/0/1 とグローバルで有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp config-digest-snooping

[AP-GigabitEthernet1/0/1] quit

[AP] stp global config-digest-snooping

関連コマンド

- **display stp**
- **stp config-digest-snooping**

4.1.23 stp global enable

Syntax

stp global enable

undo stp global enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp global enable コマンドはスパニングツリー機能をグローバルで有効にします。

undo stp global enable コマンドはスパニングツリー機能をグローバルで無効にします。

スパニングツリー機能を有効にしたとき、スパニングツリーのモードの設定により装置は STP、RSTP、MSTP モードで動作します。

スパニングツリー機能が有効であるとき、装置は受信した configuration BPDU にもとづいて VLAN のスパニングツリーの状態を維持します。スパニングツリー機能が無効であるとき、装置はスパニングツリーの状態の維持を停止します。

例

スパニングツリー機能をグローバルで有効にします。

<AP> system-view

[AP] stp global enable

関連コマンド

- **stp enable**
- **stp mode**

4.1.24 stp global mcheck

Syntax

stp global mcheck

View

System view

定義済みユーザロール

network-admin

説明

stp global mcheck コマンドはグローバルで mCheck を実行します。

MSTP、RSTP のポートが STP 装置に接続し、STP BPDU を受信すると、ポートは自動で STP モードに遷移します。しかし以下の状況ではポートは自動でもとのモードに戻ることができません。

- ピアの STP 装置がシャットダウンあるいは削除されたとき。
- ポートが変更を検出できないとき。

この場合、mCheck を実行して、ポートをもとのモードに強制的に移行させることができます。

スパニングツリーのモードの設定により装置は STP、RSTP、MSTP モードで動作します。

装置が MSTP、RSTP モードで動作しているときのみ **stp global mcheck** コマンドが適用されます。

例

グローバルで mCheck を実行します。

<AP> system-view

[AP] stp global mcheck

関連コマンド

- **stp mcheck**
- **stp mode**

4.1.25 stp loop-protection

Syntax

stp loop-protection

undo stp loop-protection

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp loop-protection コマンドはポートのループガード機能を有効にします。

undo stp loop-protection コマンドはポートのループガード機能を無効にします。

ポートのループガード機能はルートガード機能あるいは Edge ポートの設定を同時に設定することはできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 のループガード機能を有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp loop-protection

関連コマンド

- **stp edged-port**
- **stp root-protection**

4.1.26 stp max-hops

Syntax

stp max-hops *hops*

undo stp max-hops

デフォルト

20

View

System view

定義済みユーザロール

network-admin

パラメータ

hops: 最大ホップ数を設定します。設定範囲は 1〜40 です。

説明

stp max-hops コマンドは MST リージョンの最大ホップ数を設定します。

undo stp max-hops コマンドはデフォルトに戻します。

例

MST リージョンの最大ホップ数を 35 に設定します。

<AP> system-view

[AP] stp max-hops 35

関連コマンド

display stp

4.1.27 stp mcheck

Syntax

stp mcheck

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp mcheck コマンドはポートで mCheck を実行します。

MSTP、RSTP のポートが STP 装置に接続し、STP BPDU を受信すると、ポートは自動で STP モードに遷移します。しかし以下の状況ではポートは自動でもとのモードに戻ることができません。

- ピアの STP 装置がシャットダウンあるいは削除されたとき。
- ポートが変更を検出できないとき。

この場合、mCheck オペレーションを実行して、ポートをもとのモードに強制的に移行させることができます。

たとえば、デバイス A、デバイス B、デバイス C が一列に接続されています。デバイス A は STP を動作し、デバイス B はスパニングツリープロトコルが動作しておらず、デバイス C は RSTP、MSTP で動作します。デバイス C がデバイス B から透過的に転送された STP BPDU を受信すると、受信したポートは STP モードに遷移します。デバイス B をデバイス C と RSTP、MSTP で動作するように設定した場合、デバイス B とデバイス C に接続しているポートで mCheck を実行します。

スパニングツリーのモードの設定により装置は STP、RSTP、MSTP モードで動作します。

装置が MSTP、RSTP モードで動作しているときのみ **stp mcheck** コマンドが適用されます。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 で mCheck を実行します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp mcheck

関連コマンド

- **stp global mcheck**
- **stp mode**

4.1.28 stp mode

Syntax

stp mode { **mstp** | **rstp** | **stp** }

undo stp mode

デフォルト

mstp

View

System view

定義済みユーザロール

network-admin

パラメータ

mstp: MSTP モードで動作するように設定します。

rstp: RSTP モードで動作するように設定します。

stp: STP モードで動作するように設定します。

説明

stp mode コマンドはスパニングツリーの動作モードを設定します。

undo stp mode コマンドはデフォルトに戻します。

MSTP モードは RSTP モードと互換性があります。RSTP モードは STP モードと互換性があります。

例

スパニングツリーの動作モードを STP に設定します。

<AP> system-view

[AP] stp mode stp

関連コマンド

- **stp enable**
- **stp global enable**
- **stp global mcheck**
- **stp mcheck**

4.1.29 stp no-agreement-check

Syntax

stp no-agreement-check

undo stp no-agreement-check

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp no-agreement-check コマンドはポートの No Agreement Check（高速切り替え）機能を有効にします。

undo stp no-agreement-check コマンドはポートの No Agreement Check（高速切り替え）機能を無効にします。

このコマンドはルートポートでのみ有効です。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 の No Agreement Check（高速切り替え）機能を有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp no-agreement-check

4.1.30 stp pathcost-standard

Syntax

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

デフォルト

legacy

View

System view

定義済みユーザロール

network-admin

パラメータ

dot1d-1998: IEEE 802.1d-1998 規格にもとづいて、ポートのデフォルトパスコストを計算します。

dot1t: IEEE 802.1t 規格にもとづいて、ポートのデフォルトパスコストを計算します。

legacy: 独自の規格にもとづいて、ポートのデフォルトパスコストを計算します。

説明

stp pathcost-standard コマンドはポートのデフォルトパスコストを計算するときに使用する装置の規格を指定します。

undo stp pathcost-standard コマンドはデフォルトに戻します。

装置がデフォルトパスコストの計算に使用する規格を変更すると、ポートパスコストの値はデフォルトに戻ります

例

IEEE 802.1d-1998 規格にもとづいて、ポートのデフォルトパスコストを計算するように設定します。

<AP> system-view

[AP] stp pathcost-standard dot1d-1998

関連コマンド

- **display stp**
- **stp cost**

4.1.31 stp point-to-point

Syntax

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

デフォルト

デフォルトは auto で、スパニングツリーの装置は自動でポートがポイントツーポイントのリンクに接続するかどうか検出します。

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

auto: リンクタイプの自動検出を指定します。

force-false: 非ポイントツーポイントのリンクタイプを指定します。

force-true: ポイントツーポイントのリンクタイプを指定します。

説明

stp point-to-point コマンドはポートのリンクタイプを設定します。

undo stp point-to-point コマンドはデフォルトに戻します。

非ポイントツーポイントリンクに接続している場合、ポートは高速でステート遷移することはできません。

現在のポートがアグリゲートインタフェースあるいは full モードで動作しているポートである場合、ポートをポイントツーポイントリンクとしてリンクタイプを設定することができます。装置が自動でリンク状態を検出するよう、デフォルト設定を使用することを推奨します。

MSTP モードで **stp point-to-point force-false** コマンドあるいは **stp point-to-point force-true** コマンドが設定されたポートはすべての MSTI あるいは VLAN で有効です。

ポートに接続している物理的リンクがポイントツーポイントリンクではないとき、強制的にポイントツーポイントリンクになるよう設定した場合、一時的なループが発生することがあります。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 をポイントツーポイントリンクとして接続するよう設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp point-to-point force-true

関連コマンド

display stp

4.1.32 stp port priority

Syntax

stp [**instance** *instance-list*] **port priority** *priority*

undo stp [**instance** *instance-list*] **port priority**

デフォルト

128

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

priority: ポートのプライオリティを指定します。設定範囲は 0～240 で、16 の倍数です。（0、16、32、・・・のように設定します）

説明

stp port priority コマンドはポートのプライオリティを設定します。ポートのプライオリティはスパニングツリーのポートの役割に影響します。

undo stp port priority コマンドはデフォルトに戻します。

priority を小さい値にするとポートのプライオリティが高くなります。装置上のすべてのプライオリティが同一である場合、プライオリティの値はポートインデックスに依存します。インデックスが小さいとプライオリティが高くなります。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

MSTI あるいは VLAN を指定しない場合、MSTP CIST、STP あるいは RSTP のポートのプライオリティを設定します。

例

MSTP モードで MSTI 2 の GigabitEthernet 1/0/1 のプライオリティを 16 に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp instance 2 port priority 16

関連コマンド

display stp

4.1.33 stp priority

Syntax

stp [**instance** *instance-list*] **priority** *priority*

undo stp [**instance** *instance-list*] **priority**

デフォルト

32768

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

priority: 装置のプライオリティを指定します。設定範囲は 0～61440 で、4096 の倍数です（0、4096、8192・・・のように設定します）。装置で 16 までプライオリティを設定することができます。プライオリティの値を小さくすると、装置のプライオリティが高くなります。

説明

stp priority コマンドは装置のプライオリティを設定します。

undo stp priority コマンドはデフォルトのプライオリティに戻します。

MSTI あるいは VLAN を指定しない場合、MSTP CIST、STP あるいは RSTP のポートのプライオリティを設定します。

例

MSTI モードで MSTI 1 の装置のプライオリティを 4096 に設定します。

<AP> system-view

[AP] stp instance 1 priority 4096

4.1.34 stp pvst-bpdu-protection

Syntax

stp pvst-bpdu-protection

undo stp pvst-bpdu-protection

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

stp pvst-bpdu-protection コマンドは PVST BPDU ガード機能を有効にします。

undo stp pvst-bpdu-protection コマンドは PVST BPDU ガード機能を無効にします。

ポートが PVST BPDU を受信する場合、MSTP が有効な装置はポートをシャットダウンします。シャットダウンしたポートは検出間隔が終了したのち、up となります。検出間隔を設定する場合、**shutdown-interval** コマンドを使用します。

例

MSTP モードで PVST BPDU ガード機能を有効にします。

<AP> system-view

[AP] stp pvst-bpdu-protection

関連コマンド

shutdown-interval（コマンドマニュアルのセクション 2 *システム管理 “装置管理”*）

4.1.35 stp region-configuration

Syntax

stp region-configuration

undo stp region-configuration

デフォルト

MST リージョンのデフォルト設定は以下です。

- 装置の MST リージョン名は装置の MAC アドレスです。
- すべての VLAN は CIST にマッピングされています。
- MSTP のリージョンレベルは 0 です。

View

System view

定義済みユーザロール

network-admin

説明

stp region-configuration コマンドは MST region view に移行します。

undo stp region-configuration コマンドはデフォルトの MST リージョンの設定に戻します。

MST region view に移行した後、リージョン名、VLAN-インスタンスマッピング、レビジョンレベルを含む MST リージョンのパラメータを設定することができます。

例

MST region view に移行します。

<AP> system-view

[AP] stp region-configuration

[AP-mst-region]

4.1.36 stp root primary

Syntax

stp [**instance** *instance-list*] **root primary**

undo stp [**instance** *instance-list*] **root**

デフォルト

装置はルートブリッジではありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0～4094 です。0 は CIST を示します。

説明

stp root primary コマンドは装置をルートブリッジとして設定します。

undo stp root コマンドはデフォルトに戻します。

装置をルートブリッジに指定した後は、装置のプライオリティを変更することはできません。

MSTI あるいは VLAN を指定しない場合、装置を MSTP CIST、STP あるいは RSTP のルートブリッジとして設定します。

例

MSTP モードで MSTI 1 のルートブリッジとして装置を指定します。

<AP> system-view

[AP] stp instance 1 root primary

関連コマンド

- **stp priority**
- **stp root secondary**

4.1.37 stp root secondary

Syntax

stp [**instance** *instance-list*] **root secondary**

undo stp [**instance** *instance-list*] **root**

デフォルト

装置はセカンダリルートブリッジではありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

instance *instance-list*: MSTI を指定します。半角スペースで区切り 10 まで設定するか、MSTI の範囲で設定することができます。MSTI を範囲で指定する形式は *instance-id1* [**to** *instance-id2*]です。*instance-id2* は *instance-id1* 以上の値にしてください。設定範囲は 0 ～4094 です。0 は CIST を示します。

説明

stp root secondary コマンドは装置をセカンダリルートブリッジとして設定します。

undo stp root コマンドはデフォルトに戻します。

装置をルートブリッジに指定した後は、装置のプライオリティを変更することはできません。

MSTI あるいは VLAN を指定しない場合、装置を MSTP CIST、STP あるいは RSTP のセカンダリルートブリッジとして設定します。

例

MSTP モードで MSTI 1 のセカンダリルートブリッジとして装置を指定します。

<AP> system-view

[AP] stp instance 1 root secondary

関連コマンド

- **stp priority**
- **stp root primary**

4.1.38 stp root-protection

Syntax

stp root-protection

undo stp root-protection

デフォルト

無効

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

定義済みユーザロール

network-admin

説明

stp root-protection コマンドはポートでルートガード機能を有効にします。

undo stp root-protection コマンドはポートでルートガード機能を無効にします。

ポートのルートガード機能はループガード機能の設定を同時に設定することはできません。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 でルートガード機能を有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp root-protection

関連コマンド

- **stp edged-port**
- **stp loop-protection**

4.1.39 stp tc-protection

Syntax

stp tc-protection

undo stp tc-protection

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

stp tc-protection コマンドは装置の TC-BPDU ガード機能を有効にします。

undo stp tc-protection コマンドは装置の TC-BPDU ガード機能を無効にします。

TC-BPDU ガードを有効にすると、最初に TC-BPDU を受信した後、10 秒ごとに、転送アドレスエントリを即座に削除する最大数を設定することができます。TC-BPDU を制限以上受信した場合、一定の期間が経過した後、装置は、転送アドレスエントリを削除します。これにより、頻繁に転送アドレスエントリの削除を行うことを防ぐことができます。

例

装置の TC-BPDU ガード機能を無効にします。

<AP> system-view

[AP] undo stp tc-protection

関連コマンド

stp tc-protection threshold

4.1.40 stp tc-protection threshold

Syntax

stp tc-protection threshold *number*

undo stp tc-protection threshold

デフォルト

6

View

System view

定義済みユーザロール

network-admin

パラメータ

number: TC-BPDU を受信した直後から、10 秒ごとに装置が即座に転送アドレスエントリを削除する最大の回数を指定します。設定範囲は 1～255 です。

説明

stp tc-protection threshold コマンドは TC-BPDU を受信した直後から 10 秒ごとに、装置が即座に転送アドレスエントリを削除する最大の回数を設定します。

undo stp tc-protection threshold コマンドはデフォルトに戻します。

例

10 秒ごとに装置が即座に転送アドレスエントリを削除する最大の回数を 10 に設定します。

<AP> system-view

[AP] stp tc-protection threshold 10

関連コマンド

stp tc-protection

4.1.41 stp timer forward-delay

Syntax

stp [**vlan** *vlan-id-list*] **timer forward-delay** *time*

undo stp [**vlan** *vlan-id-list*] **timer forward-delay**

デフォルト

1500 センチ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id-list*: VLAN を指定します。半角スペースで区切り 10 まで設定するか、VLAN の範囲で設定することができます。VLAN を範囲で指定する形式は *vlan-id1* [**to** *vlan-id2*] です。*vlan-id2* は *vlan-id1* 以上の値にしてください。設定範囲は 1～4094 です。STP、RSTP、MSTP では使用しません。

time: 転送遅延を設定します。単位はセンチ秒です。設定範囲は 400～3000 で、100 の倍数です。（400、500、600、・・・のように設定します）

説明

stp timer forward-delay コマンドは転送遅延タイマを設定します。

undo stp timer forward-delay コマンドはデフォルトに戻します。

転送遅延タイマは状態の遷移の時間間隔を決定します。一時的なループを防ぐため、スパニングツリーのポートは廃棄状態から転送状態に遷移する前に、学習（中間）状態になります。リモート装置と同期を維持するため、ポートは転送遅延タイマの間、状態遷移を待ちます。

stp bridge-diameter コマンドでスイッチネットワークのダイアメータを指定し、**stp timer forward-delay** コマンドで転送遅延を設定しないことを推奨します。

この **stp bridge-diameter** コマンドによってスパニングツリーは転送遅延タイマを最適な値に自動で計算します。ネットワークダイアメータがデフォルト値である場合、転送遅延タイマもデフォルト値を使用します。

例

MSTP モードで転送遅延タイマを 2000 センチ秒に設定します。

<AP> system-view

[AP] stp timer forward-delay 2000

関連コマンド

- **stp bridge-diameter**
- **stp timer hello**
- **stp timer max-age**

4.1.42 stp timer hello

Syntax

stp timer hello *time*

undo stp timer hello

デフォルト

200 センチ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time: hello 時間を設定します。単位はセンチ秒です。設定範囲は 100～1000 で、100 の倍数です。（100、200、300、・・・のように設定します）

説明

stp timer hello コマンドは hello 時間を設定します。

undo stp timer hello コマンドはデフォルトに戻します。

hello 時間はスパニングツリーを維持するため、装置が configuration BPDU を送信する間隔です。装置が指定した時間以内に configuration BPDU を受信できない場合、新たなスパニングツリー計算が開始されます。

stp bridge-diameter コマンドでスイッチネットワークのダイアメータを指定し、**stp timer hello** コマンドで hello 時間を設定しないことを推奨します。

この **stp bridge-diameter** コマンドによってスパニングツリーは hello 時間を最適な値に自動で計算します。ネットワークダイアメータがデフォルト値である場合、hello 時間もデフォルト値を使用します。

例

MSTP モードで hello 時間を 400 センチ秒に設定します。

<AP> system-view

[AP] stp timer hello 400

関連コマンド

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer max-age**

4.1.43 stp timer max-age

Syntax

stp timer max-age *time*

undo stp timer max-age

デフォルト

2000 センチ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time: 最大エージングタイマを設定します。単位はセンチ秒です。設定範囲は 600～4000 で、100 の倍数です。（600、700、800、・・・のように設定します）

説明

stp timer max-age コマンドは装置の最大エージングタイマを設定します。

undo stp timer max-age コマンドはデフォルトに戻します。

MSTP ネットワークの CIST で、装置は最大エージングタイマにもとづいて、ポートが受信した configuration BPDU がタイムアウトしているかどうかを判断します。ポートで configuration BPDU の受信がタイムアウトした場合、新しいスパニングツリーの再計算が開始されます。最大エージングタイマは、CIST（あるいは MSTI 0）のみ有効です。

stp bridge-diameter コマンドでスイッチネットワークのダイアメータを指定し、**stp timer max-age** コマンドで最大エージングタイマを設定しないことを推奨します。

この **stp bridge-diameter** コマンドによってスパニングツリーは最大エージングタイマを最適な値に自動で計算します。ネットワークダイアメータがデフォルト値である場合、最大エージングタイマもデフォルト値を使用します。

例

MSTP モードで最大エージングタイマを 1000 センチ秒に設定します。

<AP> system-view

[AP] stp timer max-age 1000

関連コマンド

- **stp bridge-diameter**
- **stp timer forward-delay**
- **stp timer hello**

4.1.44 stp timer-factor

Syntax

stp timer-factor *factor*

undo stp timer-factor

デフォルト

3

View

System view

定義済みユーザロール

network-admin

パラメータ

factor: タイムアウトファクタを指定します。設定範囲は 1～20 です。

説明

stp timer-factor コマンドはタイムアウト時間を決めるタイムアウトファクタを設定します。

タイムアウト時間＝タイムアウトファクタ×3×hello 時間

undo stp timer-factor コマンドはデフォルトに戻します。

ネットワークトポロジが安定した後、各非ルートブリッジは、リンク異常を確認するために周囲の装置に対し、hello 時間の間隔で設定 BPDU を転送します。通常、装置が上流装置から hello 時間の 9 倍の時間内に BPDU を受信しないと、装置は上流装置が故障しているとみなし、新たなスパニングツリー計算を開始します。

安定したネットワークにおいては、このようなスパニングツリー計算は、上流装置がビジー状態の場合に起こります。この場合、タイムアウト時間を長く（4 以上に）設定することにより、このような不要なスパニングツリー計算を避け、ネットワークリソースを節約できます。安定したネットワークでは、タイムアウトファクタを 5、6、または 7 に設定することが推奨されます。

例

タイムアウトファクタを 7 に設定します。

<AP> system-view

[AP] stp timer-factor 7

関連コマンド

stp timer hello

4.1.45 stp transmit-limit

Syntax

stp transmit-limit *limit*

undo stp transmit-limit

デフォルト

すべてのポートの BPDU の転送レートは 10 です。各ポートは各 hello 時間内に 10 の BPDU を送信します。

View

Layer 2 Ethernet interface view, Layer 2 aggregate interface view

定義済みユーザロール

network-admin

パラメータ

limit: BPDU 転送レートを設定します。設定範囲は 1～255 です。

説明

stp transmit-limit コマンドはポートの BPDU 転送レートを設定します。

undo stp transmit-limit コマンドはデフォルトに戻します。

各 hello 時間以内にポートが送信できる BPDU の最大数は、BPDU 転送レートと hello 時間の合計に等しいです。

BPDU 転送レートを大きくするとは多くのシステムリソースが必要となります。

最大 BPDU 転送レートを適切に設定することにより、ポートが BPDU を送信するスピードを制限し、ネットワークトポロジが変更した際に過剰な帯域リソースを使用しないようにできます。デフォルト値を使うことを推奨します。

interface view で設定を行うと、設定は、現在のインタフェースでのみ有効になります。

aggregate interface view で設定を行うと、設定はアグリゲートインタフェースでのみ有効になります。

アグリゲーショングループのメンバポートで設定を行うと、ポートがアグリゲーショングループを除外した後に有効になります。

例

GigabitEthernet 1/0/1 の BPDU 転送レートを 5 に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] stp transmit-limit 5

4.1.46 vlan-mapping modulo

Syntax

vlan-mapping modulo *modulo*

デフォルト

すべての VLAN は CIST（MSTI 0）にマッピングされています。

View

MST region view

定義済みユーザロール

network-admin

パラメータ

modulo: モジュロの値を設定します。設定範囲は 1～64 です。

説明

vlan-mapping modulo コマンドは指定モジュロの値に従って MST リージョンの VLAN を MSTI にマッピングし、VLAN インスタンスマッピングテーブルの作成を早急に行います。

異なる MSTI に VLAN をマッピングすることはできません。すでに MSTI にマッピングされている VLAN を新しい MSTI にマッピングすると、古いマッピングは自動的に削除されます。

このコマンドは、次の式に従い、VLAN をマッピングする MSTI の ID を決定します。

ID ＝ (VLAN ID － 1) %*modulo* ＋ 1

(VLAN ID － 1) %*modulo* は (VLAN ID － 1)に対してモジュロ演算を行うことを意味します。モジュロの値が 15 である場合、VLAN 1 は MSTI 1 に、VLAN 2 は MSTI 2 に、VLAN 15 は MSTI 15 に、VLAN 16 は MSTI 16 のようにマッピングされます。

例

VLAN を MSTI にモジュロ 8 でマッピングします。

<AP> system-view

[AP] stp region-configuration

[AP-mst-region] vlan-mapping modulo 8

関連コマンド

- **active region-configuration**
- **check region-configuration**
- **display stp region-configuration**
- **region-name**

- **revision-level**

目次

このセクションのページは **4-x-x** です。

5 章 LLDP 5-1
5.1 LLDP 設定コマンド 5-1
5.1.1 display lldp local-information 5-1
5.1.2 display lldp neighbor-information 5-6
5.1.3 display lldp statistics 5-12
5.1.4 display lldp status 5-15
5.1.5 display lldp tlv-config 5-18
5.1.6 lldp admin-status 5-22
5.1.7 lldp check-change-interval 5-23
5.1.8 lldp enable 5-24
5.1.9 lldp encapsulation snap 5-25
5.1.10 lldp fast-count 5-26
5.1.11 lldp global enable 5-27
5.1.12 lldp hold-multiplier 5-28
5.1.13 lldp management-address-format string 5-29
5.1.14 lldp notification remote-change enable 5-30
5.1.15 lldp timer notification-interval 5-31
5.1.16 lldp timer reinit-delay 5-32
5.1.17 lldp timer tx-interval 5-32
5.1.18 lldp tlv-enable 5-33

5章 LLDP

5.1 LLDP設定コマンド

5.1.1 display lldp local-information

Syntax

display lldp local-information [**global** | **interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルのローカル LLDP 情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display lldp local-information コマンドはローカル LLDP 情報を表示します。

パラメータを指定しない場合、以下が含まれるすべてのローカル LLDP 情報を表示します。

- グローバルの LLDP 情報
- up 状態の LLDP が有効なポートの LLDP 情報

例

すべてのローカル LLDP 情報を表示します。

<AP> display lldp local-information

```
Global LLDP local-information:
 Chassis ID         : 307b-ac6c-4cc0
 System name        : AP
   System description  :
    Comware Platform Software, Software Version 7.5.114, 7.5.114
    NEC QX-W610
 System capabilities supported : Bridge, WlanAccessPoint, Router, Customer Bridg
                                 e, Service Bridge
 System capabilities enabled   : Bridge, Router, Customer Bridge
```

```
MED information:
Device class             : Connectivity device
HardwareRev              : Ver.A
FirmwareRev              : 1.03
SoftwareRev              : 7.5.114
SerialNum                : 219801A4M1P243XXXXXX
Manufacturer name         : NEC
Model name               : QX-W610
Asset tracking identifier  : Unknown
```

表 5-1 コマンド出力

フィールド	説明
Chassis ID	装置のBridge MACアドレスです。
System capabilities supported	サポートされる機能です。 ● **Bridge**–スイッチングがサポートされます。 ● **Router**–ルーティングがサポートされます。 ● **Customer Bridge**–カスタマブリッジ機能がサポートされます。 ● **Service Bridge**–サービスブリッジ機能がサポートされます。
System capabilities enabled	有効な機能です。 ● **Bridge**–スイッチングが有効です。 ● **Router**–ルーティングが有効です。 ● **Customer Bridge**–カスタマブリッジ機能が有効です。 ● **Service Bridge**–サービスブリッジ機能が有効です。
Device class	MED装置のクラスです。 ● **Connectivity device**–ネットワーク装置です。 ● **Class I**–通常の端末装置です。basic LLDP検出サービスが必要です。 ● **Class II**–メディア端末装置です。通常の端末装置に加えて、メディアストリームをサポートします。 ● **Class III**–通信端末装置です。通常の端末装置、メディアストリームに加えて、エンドユーザのIP通信システムをサポートします。
MED inventory information of master board	MEDインベントリに関する情報です。
HardwareRev	ハードウェアバージョンです。

フィールド	説明
FirmwareRev	ファームウェアバージョンです。
SoftwareRev	ソフトウェアバージョンです。
SerialNum	シリアル番号です。
Manufacturer name	装置の製造メーカです。
Model name	装置モデルです。
Port ID type	ポートIDタイプです。 ● MACアドレスです。 ● インタフェース名です。
Port ID	ポートIDです。ポートIDタイプによって変わります。
Management address interface type	管理アドレスで識別されるインタフェースの番号タイプです。
Management address interface ID	管理アドレスで識別されるインタフェースのインデックスです。
Management address OID	管理アドレスのオブジェクトIDです。
Port VLAN ID(PVID)	
Port and protocol VLAN ID(PPVID)	
Port and protocol VLAN supported	
Port and protocol VLAN enabled	
Link aggregation supported	ポートのリンクアグリゲーションがサポートされているかどうかを示します。
Link aggregation enabled	ポートのリンクアグリゲーションが有効かどうかを示します。
Aggregation port ID	メンバポートIDです。リンクアグリゲーションが無効であるとき、0と表示されます。
Auto-negotiation supported	ポートのオートネゴシエーションがサポートされているかを示します。
Auto-negotiation enabled	ポートのオートネゴシエーションが有効かどうかを示します。
OperMau	ポートの通信速度、通信モードです。
Power port class	PoEポートのクラスです。 ● **PSE**−電力供給装置です。

フィールド	説明
	• **PD**–電力が供給された装置です。
PSE power supported	装置がPSEとして動作可能かどうかを示します。
PSE power enabled	装置がPSEとして動作しているかどうかを示します。
PSE pairs control ability	PSE-PD間のPoE電力管理機能が有効かどうかを示します。
Power pairs	電力供給モードです。 • **Signal**–データ転送と同時に電力を供給します。 • **Spare**–データ転送と別の信号線で電力を供給します。
Port power classification	PDのポート供給電力のクラスです。この表示は、PSEが供給できるPDの供給電力のクラスを表しており、PSE装置でない場合は未対応です。PSE装置でない場合は、"Class 0"を表示します。 • **Class 0**ークラス0です。 • **Class 1**ークラス1です。 • **Class 2**ークラス2です。 • **Class 3**ークラス3です。 • **Class 4**ークラス4です。

Power source	電源:
	• 電源の種類がPSEの場合、オプションは次のとおりです。
	  • Unknown—不明な電源です。
	  • Primary—プライマリ電源です。
	  • Backup—バックアップ電源です。
	  • Reserved
	• 電源の種類がPDの場合、オプションは次のとおりです。
	  • Unknown—不明な電源です。
	  • PSE—PSE電源です。
	  • Local—ローカル電源です。
	  • PSE and local—PSE電源とローカル電源です。

Power PD priority	PDポートのPoE電力受信優先度です。 • Unknown • Critical • High • Low
Transmit Tw	ローカルクライアントのスリープ時間です。単位はμsです。

フィールド	説明
Receive Tw	ローカルクライアントによって予期されたピアのクライアントのスリープ時間です。単位はμsです。
Port available power value	PSEポートのPoE電力あるいはPDポートで必要な電力です。単位はWです。
Echo Transmit Tw	ピアのクライアントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 • ローカルクライアントがピアクライアントのスリープ時間を受信していません。 • ピアクライアントのスリープ時間は0μsです。
Echo Receive Tw	ピアのクライアントによって予期されたローカルクライアントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 • ローカルクライアントがピアのクライアントから予期されたスリープ時間を受信していません。 • ピアのクライアントによって予期されたローカルクライアントのスリープ時間が0μsです。

5.1.2 display lldp neighbor-information

Syntax

display lldp neighbor-information [[[**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }] [**verbose**]] | **list** [**system-name** *system-name*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、隣接装置から受信するすべてのポートの LLDP 情報を表示します。

agent: エージェント種別を指定します。エージェント種別を指定しない場合、すべての LLDP エージェントが近隣装置から受信する LLDP 情報を表示します。

nearest-bridge: 最も近いブリッジエージェントを指定します。

nearest-customer: 最も近いカスタマーブリッジエージェントを指定します。

nearest-nontpmr: 最も近い非 TPMR ブリッジエージェントを指定します。

verbose: ローカル装置が隣接装置から受信する LLDP の詳細情報を表示します。指定しない場合、ローカル装置が隣接装置から受信する LLDP の概要情報を表示します。

list: ローカル装置が隣接装置から受信する LLDP の情報をリスト形式で表示します。

system-name *system-name*: システム名で指定された隣接装置からローカル装置が受信する LLDP の情報を表示します。設定範囲は 1～255 です。指定しない場合、リストのすべての隣接装置からローカル装置が受信する LLDP の情報を表示します。

説明

display lldp neighbor-information コマンドはローカル装置が隣接装置から受信する LLDP 情報を表示します。LLDP 情報は LLDP TLV として受信します。

例

隣接装置からすべてのポートのすべての LLDP エージェントが受信した LLDP の詳細情報を表示します。

<AP> display lldp neighbor-information verbose

```
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
```

```
 Update time        : 0 days, 0 hours, 0 minutes, 40 seconds
 Chassis type       : MAC address
 Chassis ID         : 9c06-1b97-9272
 Port ID type       : Interface name
 Port ID           : GigabitEthernet1/0/1
 Time to live       : 120
 Port description    : GigabitEthernet1/0/1 Interface
 System name        : QX-L2-SW2
 System description  : QX-S1016GT-4G-PW Software Version 5.2.8
...
```

隣接装置からすべてのポートのすべての LLDP エージェントが受信した LLDP の概要情報を表示します。

<AP> display lldp neighbor-information

```
LLDP neighbor-information of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
 LLDP neighbor index : 1
 ChassisID/subtype   : 9c06-1b97-9272/MAC address
 PortID/subtype      : GigabitEthernet1/0/1/Interface name
 Capabilities       : Bridge, Router
```

隣接装置からすべての LLDP エージェントが受信した LLDP の概要情報をリスト形式で表示します。

<AP> display lldp neighbor-information list

```
Chassis ID : * -- -- Nearest nontpmr bridge neighbor
           # -- -- Nearest customer bridge neighbor
           Default -- -- Nearest bridge neighbor
System Name         Local Interface Chassis ID     Port ID
QX-L2-SW2           GE1/0/1        9c06-1b97-9272  GigabitEthernet1/0/1
```

表 5-2 コマンド出力

フィールド	説明
LLDP neighbor-information of port 1	LLDP情報がポート1から受信されました。
Update time	隣接情報のLLDP情報が最後にアップデートされた時間です。
Chassis type	装置IDタイプです。 • **Chassis component**－装置構成です。 • **Interface alias**－インタフェースの通称です。 • **Port component**－ポート構成です。 • **MAC address**－MACアドレスです。 • **Network address (ipv4)**－ネットワークアドレスです。

フィールド	説明
	（IPv4） • **Interface name**－インタフェース名です。 • **Locally assigned**–上記にリストされたタイプ以外のローカルで定義された装置タイプです。
Chassis ID	LLDPが送信する装置を識別するIDです。 MACアドレス、ネットワークアドレス、インタフェース、あるいはそれ以外の値を使用することができ、隣接装置の装置タイプに依存します。
Port ID type	ポートIDタイプです。 • **Interface alias**－インタフェースの通称です。 • **Port component**－ポート構成です。 • **MAC address**－MACアドレスです。 • **Network address (ipv4)**－ネットワークアドレスです。（IPv4） • **Interface name**－インタフェース名です。 • **Agent circuit ID**－エージェントcircuit IDです。 • **Locally assigned**–上記にリストされたタイプ以外のローカルで定義されたポートIDタイプです。
Port ID	ポートIDのタイプの値です。
System name	隣接装置のシステム名です。
System description	隣接装置のシステムの説明です。
System capabilities supported	隣接装置でサポートされる機能です。 • **Repeater**–信号のリピータがサポートされます。 • **Bridge**–スイッチングがサポートされます。 • **WlanAccessPoint**–隣接装置は、無線APとして機能します。 • **Router**–ルーティングがサポートされます。 • **Telephone**–隣接装置が電話として動作できます。 • **DocsisCableDevice**–隣接装置がDOCSIS準拠のケーブル装置として動作します。 • **StationOnly**–隣接装置が基地局のみとして動作します。 • **Customer Bridge**–カスタマブリッジ機能がサポートされます。 • **Service Bridge**–サービスブリッジ機能がサポートされます。 • **TPMR**– TPMR（The two-port MAC relay）機能がサポートされます。

フィールド	説明
	• **Other**–上記で記載されている以外の機能がサポートされます。
System capabilities enabled	隣接装置で有効な機能です。 • **Repeater**–信号のリピータが有効です。 • **Bridge**–スイッチングが有効です。 • **WlanAccessPoint**–隣接装置は、無線APとして機能します。 • **Router**–ルーティングが有効です。 • **Telephone**–隣接装置が電話として動作できます。 • **DocsisCableDevice**–隣接装置がDOCSIS準拠のケーブル装置として動作しています。 • **StationOnly**–隣接装置が基地局のみとして動作しています。 • **Customer Bridge**–カスタマブリッジ機能が有効です。 • **Service Bridge**–サービスブリッジ機能が有効です。**TPMR**–TPMR（The two-port MAC relay）機能が有効です。 • **Other**–上記で記載されている以外の機能が有効です。
Management address OID	管理アドレスのオブジェクトIDです。
Port and protocol VLAN ID(PPVID)	ポートのプロトコルVLAN IDです。
Port and protocol VLAN supported	ポートのプロトコルVLANがサポートされているかどうかを示します。
Port and protocol VLAN enabled	ポートのプロトコルVLANが有効かどうかを示します。
VLAN name of VLAN 12	VLAN 12の名前です。
Aggregation port ID	メンバポートIDです。リンクアグリゲーションが無効であるとき、0と表示されます。
Auto-negotiation supported	ポートでネゴシエーションがサポートされているかを示します。
Auto-negotiation enabled	ポートでネゴシエーションが有効かどうかを示します。
OperMau	ポートの通信速度と通信モードの状態です。
Power port class	PoEポートのクラスです。 • **PSE**–電力供給装置です。 • **PD**–電力が供給された装置です。
PSE power supported	装置がPSEとして動作可能かどうかを示します。
PSE power enabled	装置がPSEとして動作しているかどうかを示します。

フィールド	説明
PSE pairs control ability	PSE-PD間のPoE電力管理機能が有効かどうかを示します。
Power pairs	電力供給モードです。 ● **Signal**–データ転送と同時に電力を供給します。 ● **Spare**–データ転送と別の信号線で電力を供給します。
Port power classification	PDのポート供給電力のクラスです。 ● **Class 0**ークラス0です。 ● **Class 1**ークラス1です。 ● **Class 2**ークラス2です。 ● **Class 3**ークラス3です。 ● **Class 4**ークラス4です。
PSE powering status	PSEの電源状態です。 ● **Reserved**—不明な電源状態 ● **2-pair powering**— 2ペア電源モード ● **4-pair powering single**—単一シグニチャPDの4ペア電源モード ● **4-pair powering dual-signature PD**—二重シグニチャPDの4ペア電源モード
Capabilities	隣接装置で有効な機能です。 ● **Repeater**–信号のリピータが有効です。 ● **Bridge**–スイッチングが有効です。
Local Interface	LLDP情報を受信するローカルポートです。
Chassis ID : * -- -- Nearest nontpmr bridge neighbor #-- -- Nearest customer bridge neighbor	シャーシIDのフラグです。 ● （*）はnearest non-TPMR bridge neighborを示します。 ● （#）はnearest customer bridge neighborを示します。
Transmit Tw	ローカルクライアントのスリープ時間です。単位はμsです。
Receive Tw	ローカルクライアントによって予期されたピアのクライアントのスリープ時間です。単位はμsです。
Fallback Tw	ローカルクライアントによって予期されたピアのクライアント候補のスリープ時間です。単位はμsです。
Echo Transmit Tw	ピアのクライアントのスリープ時間です。単位はμsです。このフィールドは以下の場合、0と表示されます。 ● ローカルクライアントがピアのクライアントのスリープ時間を受信していません。 ● ピアのクライアントのスリープ時間が0μsです。
Echo Receive Tw	ピアのクライアントによって予期されたローカルクライア

フィールド	説明
	ントのスリープ時間です。単位はμsです。 このフィールドは以下の場合、0と表示されます。 • ローカルクライアントがピアのクライアントから予期されたスリープ時間を受信していません。 • ピアのクライアントによって予期されたローカルクライアントのスリープ時間が0μsです。

5.1.3 display lldp statistics

Syntax

display lldp statistics [**global** | [**interface** *interface-type interface-number*]] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

global: グローバルの LLDP の統計情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

agent: エージェント種別を指定します。エージェント種別を指定しない場合、すべての LLDP エージェントが近隣装置から受信する LLDP 情報を表示します。

nearest-bridge: 最も近いブリッジエージェントを指定します。

nearest-customer: 最も近いカスタマーブリッジエージェントを指定します。

nearest-nontpmr: 最も近い非 TPMR ブリッジエージェントを指定します。

説明

display lldp statistics コマンドはグローバルあるいはポートの LLDP の統計情報を表示します。

キーワードを指定しない場合、グローバルの LLDP の統計情報とすべてのポートの LLDP の統計情報を表示します。

例

グローバルの LLDP の統計情報とすべてのポートの LLDP の統計情報を表示します。

<AP> display lldp statistics

```
LLDP statistics global information:
LLDP neighbor information last change time:0 days, 0 hours, 0 minutes, 40 seconds
The number of LLDP neighbor information inserted : 1
The number of LLDP neighbor information deleted  : 0
The number of LLDP neighbor information dropped  : 0
The number of LLDP neighbor information aged out : 0

LLDP statistics information of port 1 [GigabitEthernet1/0/1]:
```

```
LLDP agent nearest-bridge:
The number of LLDP frames transmitted          : 10
The number of LLDP frames received             : 5
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP agent nearest-nontpmr:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0

LLDP agent nearest-customer:
The number of LLDP frames transmitted          : 0
The number of LLDP frames received             : 0
The number of LLDP frames discarded            : 0
The number of LLDP error frames                : 0
The number of LLDP TLVs discarded              : 0
The number of LLDP TLVs unrecognized           : 0
The number of LLDP neighbor information aged out : 0
The number of CDP frames transmitted           : 0
The number of CDP frames received              : 0
The number of CDP frames discarded             : 0
The number of CDP error frames                 : 0
```

表 5-3 コマンド出力

フィールド	説明
LLDP statistics global information	グローバルのLLDPの統計情報です。
LLDP neighbor information last change time	隣接情報が最後にアップデートした時間です。
The number of LLDP neighbor information inserted	隣接情報が追加された回数です。
The number of LLDP neighbor information deleted	隣接情報が削除された回数です。
The number of LLDP neighbor information dropped	メモリ空き容量が足りないために隣接情報が廃棄された回数です。

5.1.4 display lldp status

Syntax

display lldp status [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、グローバルの LLDP の状態とすべてのポートの LLDP の状態を表示します。

agent: エージェント種別を指定します。エージェント種別を指定しない場合、すべての LLDP エージェントが近隣装置から受信する LLDP 情報を表示します。

nearest-bridge: 最も近いブリッジエージェントを指定します。

nearest-customer: 最も近いカスタマーブリッジエージェントを指定します。

nearest-nontpmr: 最も近い非 TPMR ブリッジエージェントを指定します。

説明

display lldp status コマンドは LLDP の状態を表示します。

例

グローバルの LLDP の状態と各ポートの LLDP の状態を表示します。

<AP> display lldp status

```
Global status of LLDP: Enable
Bridge mode of LLDP: customer-bridge
The current number of LLDP neighbors: 1
The current number of CDP neighbors: 0
LLDP neighbor information last changed time: 0 days, 0 hours, 0 minutes, 40 seconds
Transmit interval            : 30s
Fast transmit interval       : 1s
Transmit max credit          : 5
Hold multiplier              : 4
Reinit delay                 : 2s
Trap interval                : 30s
Fast start times             : 4
```

```
LLDP status information of port 1 [GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
Port status of LLDP          : Enable
Admin status                 : TX_RX
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 1
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV  : 11
Number of received unknown TLV : 0

LLDP agent nearest-nontpmr:
Port status of LLDP          : Enable
Admin status                 : Disable
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV  : 0
Number of received unknown TLV : 0

LLDP agent nearest-customer:
Port status of LLDP          : Enable
Admin status                 : Disable
Trap flag                    : No
MED trap flag                : No
Polling interval             : 0s
Number of LLDP neighbors     : 0
Number of MED neighbors      : 0
Number of CDP neighbors      : 0
Number of sent optional TLV  : 0
Number of received unknown TLV : 0
```

表 5-4 コマンド出力

フィールド	説明
Bridge mode of LLDP	LLDPブリッジモードです。サービスブリッジあるいはカスタマブリッジがあります。

フィールド	説明
Global status of LLDP	LLDPがグローバルで有効かどうかを示します。
LLDP neighbor information last changed time	隣接情報が最後にアップデートされた時間です。
Transmit interval	LLDPフレームの転送間隔です。
Hold multiplier	TTL乗数です。
Reinit delay	LLDPを再初期化の遅延時間です。
Transmit max credit	LLDPフレームを送信するトークンバケットサイズです。
Trap interval	トラップを転送する間隔です。
Fast start times	新しい隣接装置が検出された際、連続して送信されるLLDPフレームの回数です。
Port 1	ポート1のLLDPの状態です。
Port status of LLDP	ポートのLLDPが有効かどうかを示します。
Admin status	ポートのLLDP動作モードです。 • **Tx_Rx**–ポートはLLDPフレームの送受信ができます。 • **Rx_Only**–ポートはLLDPフレームの受信のみができます。 • **Tx_Only**–ポートはLLDPフレームの送信のみができます。 • **Disable**–ポートはLLDPフレームの送受信ができません。
Trap Flag	トラップが有効かどうかを示します。
Polling interval	LLDPのポーリング間隔です。0はLLDPのポーリングが無効であることを示します。
Number of neighbors	ポートに接続しているLLDPの隣接数です。
Number of MED neighbors	ポートに接続しているMEDの隣接数です。
Number of CDP neighbors	ポートに接続しているCDPの隣接数です。
Number of sent optional TLV	LLDPフレームに含まれるオプションTLVがポートに送信された数です。
Number of received unknown TLV	受信されたLLDPフレームに含まれる不明なTLVの数です。

5.1.5 display lldp tlv-config

Syntax

display lldp tlv-config [**interface** *interface-type interface-number*] [**agent** { **nearest-bridge** | **nearest-customer** | **nearest-nontpmr** }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのポートで通知可能なオプション LLDP TLV のタイプを表示します。

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの動作モードを設定します。

nearest-bridge: 最も近いブリッジエージェントを指定します。

nearest-customer: 最も近いカスタマーブリッジエージェントを指定します。

nearest-nontpmr: 最も近い非 TPMR ブリッジエージェントを指定します。

説明

display lldp tlv-config コマンドはポートで通知可能なオプション LLDP TLV のタイプを表示します。

例

GigabitEthernet 1/0/1 で通知可能なオプションの LLDP TLV のタイプを表示します。

<AP> display lldp tlv-config gigabitethernet 1/0/1

```
LLDP tlv-config of port 1[GigabitEthernet1/0/1]:
LLDP agent nearest-bridge:
NAME                          STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV           YES       YES
 System Name TLV               YES       YES
 System Description TLV         YES       YES
 System Capabilities TLV        YES       YES
 Management Address TLV         YES       YES
IEEE 802.1 extend TLV:
```

```
 Port VLAN ID TLV               YES      YES
 Port And Protocol VLAN ID TLV    NO       NO
 VLAN Name TLV                 NO       NO
 DCBX TLV                      NO       NO
 EVB TLV                       NO       NO
 Link Aggregation TLV           YES      YES
 Management VID TLV             NO       NO
 Congestion notification TLV     NO       NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                YES      YES
 Power via MDI TLV             YES      YES
 Maximum Frame Size TLV         YES      YES
 Energy-Efficient Ethernet TLV    NO       NO
 LLDP-MED extend TLV:
 Capabilities TLV              YES      YES
 Network Policy TLV            YES      YES
 Location Identification TLV     NO       NO
 Extended Power via MDI TLV      YES      YES
 Inventory TLV                 YES      YES

LLDP agent nearest-nontpmr:
NAME                          STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV           NO       NO
 System Name TLV               NO       NO
 System Description TLV         NO       NO
 System Capabilities TLV        NO       NO
 Management Address TLV         NO       NO
IEEE 802.1 extend TLV:
 Port VLAN ID TLV              NO       NO
 Port And Protocol VLAN ID TLV    NO       NO
 VLAN Name TLV                 NO       NO
 DCBX TLV                      NO       NO
 EVB TLV                       YES      YES
 Link Aggregation TLV           NO       NO
 Management VID TLV             NO       NO
 Congestion notification TLV     NO       NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                NO       NO
 Power via MDI TLV             NO       NO
 Maximum Frame Size TLV         NO       NO
 Energy-Efficient Ethernet TLV    NO       NO
LLDP-MED extend TLV:
```

```
 Capabilities TLV              NO       NO
 Network Policy TLV            NO       NO
 Location Identification TLV     NO       NO
 Extended Power via MDI TLV      NO       NO
 Inventory TLV                 NO       NO

LLDP agent nearest-customer:
NAME                          STATUS    DEFAULT
Basic optional TLV:
 Port Description TLV          YES      YES
 System Name TLV               YES      YES
 System Description TLV        YES      YES
 System Capabilities TLV       YES      YES
 Management Address TLV        YES      YES
IEEE 802.1 extend TLV:
 Port VLAN ID TLV              YES      YES
 Port And Protocol VLAN ID TLV   NO       NO
 VLAN Name TLV                 NO       NO
 DCBX TLV                      NO       NO
 EVB TLV                       NO       NO
 Link Aggregation TLV          YES      YES
 Management VID TLV            NO       NO
 Congestion notification TLV     NO       NO
IEEE 802.3 extend TLV:
 MAC-Physic TLV                NO       NO
 Power via MDI TLV             NO       NO
 Maximum Frame Size TLV        NO       NO
 Energy-Efficient Ethernet TLV   NO       NO
LLDP-MED extend TLV:
 Capabilities TLV              NO       NO
 Network Policy TLV            NO       NO
 Location Identification TLV     NO       NO
 Extended Power via MDI TLV      NO       NO
 Inventory TLV                 NO       NO
```

表 5-5 コマンド出力

フィールド	説明
LLDP tlv-config of port 1	ポート1の通知可能なオプションTLVです。
NAME	TLVのタイプです。
STATUS	TLVのタイプがポートに送信されたかどうかを示します。

フィールド	説明
DEFAULT	デフォルトでTLVのタイプがポートに送信されたかどうかを示します。
Basic optional TLV	basic TLVのオプションTLVです。 ● **Port description TL**V－ポート説明TLVです。 ● **System name TLV**－システム名TLVです。 ● **System description TLV**－システム説明TLVです。 ● **System capabilities TLV**－システム機能TLVです。 ● **Management address TLV**－管理アドレスTLVです。 ● Congestion notification TLV－輻輳通知TLVです。
IEEE 802.1 extended TLV	IEEE802.1組織指定TLVです。 ● **Port VLAN ID TLV**－ポートVLAN ID TLVです。 ● **Port and protocol VLAN ID TLV**－ポートのプロトコルVLAN TLVです。 ● **VLAN name TLV**－VLAN名TLVです。 ● **DCBX TLV**－DCBX TLVです。DCBX TLVはサポートしていません。 ● **EVB TLV**－EVB TLVです。EVB TLVはサポートしていません。 ● **Management VID TLV**－管理VID TLVです。
IEEE 802.3 extended TLV	IEEE802.3組織指定TLVです。 ● **MAC-Physic TLV**－MAC物理TLVです。 ● **Power via MDI TLV**－MDI経由の電力TLVです。 ● **Link aggregation TLV**－リンクアグリゲーションTLVです。 ● **Maximum frame size TLV**－最大フレームサイズTLVです。
LLDP-MED extend TLV	LLDP-MED TLVです。 ● **Capabilities TLV**－機能TLVです。 ● **Network Policy TLV**－ネットワークポリシーTLVです。 ● **Extended Power-via-MDI TLV**－拡張MDI経由TLVです。 ● **Location Identification TLV**－位置識別TLVです。 ● **Inventory TLV**－インベントリTLVです。
Inventory TLV	インベントリTLVです。 ● **Hardware Revision TLV**－ハードウェアレビジョンTLVです。 ● **Firmware Revision TLV**－ファームウェアレビジョンTLVです。 ● **Software Revision TLV**－ソフトウェアレビジョンTLVです。 ● **Serial Number TLV**－シリアル番号TLVです。

フィールド	説明
	• **Manufacturer Name TLV**－装置の製造メーカTLVです。 • **Model name TLV**－装置名TLVです。 • **Asset ID TLV**－Asset ID TLVです。

5.1.6 lldp admin-status

Syntax

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status** { **disable** | **rx** | **tx** | **txrx** }

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **admin-status**

デフォルト

nearest bridge エージェントは txrx モード、nearest customer bridge エージェントは disable です。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントタイプを指定します。指定しない場合、nearest bridge エージェントの動作モードを設定します。

nearest-customer: 最も近いカスタマーブリッジエージェントを指定します。

nearest-nontpmr: 最も近い非 TPMR ブリッジエージェントを指定します

disable: Disable モードを指定します。Disable モードのポートは LLDP フレームの送受信ができません。

rx: Rx モードを指定します。Rx モードのポートは LLDP フレームの受信のみができます。

ポートは LLDP フレームの送受信ができます。

tx: Tx モードを指定します。Tx モードのポートは LLDP フレームの送信のみができます。

ポートは LLDP フレームの送受信ができます。

txrx: TxRx モードを指定します。TxRx モードのポートは LLDP フレームの送受信ができます。

説明

lldp admin-status コマンドは LLDP の動作モードを指定します。

undo lldp admin-status コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP 動作モードを Rx に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] lldp agent nearest-customer admin-status rx

5.1.7 lldp check-change-interval

Syntax

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval** *interval*

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **check-change-interval**

デフォルト

LLDP polling は、無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントのタイプを指定します。Ethernet interface view でエージェント タイプを指定しない場合、このコマンドは LLDP polling を有効にし、nearest bridge エージェントの polling interval を設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

nearest-nontpmr: nearest non-TPMR bridge エージェントを指定します。

interval: LLDP polling interval を 1 ～ 30 秒の範囲で設定します。

説明

lldp check-change-interval コマンドは、LLDP polling を有効にし、polling interval を設定します。

undo lldp check-change-interval コマンドは、LLDP polling を無効にします。

例

LLDP polling を有効にし、GigabitEthernet 1/0/1 の nearest customer bridge エージェントの polling interval を 30 秒に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] lldp agent nearest-customer check-change-interval 30

5.1.8 lldp enable

Syntax

lldp enable

undo lldp enable

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

lldp enable コマンドはポートで LLDP を有効にします。

undo lldp enable コマンドはポートで LLDP を無効にします。

LLDP はグローバルとポートの両方で有効にしたときのみ適用されます。

例

GigabitEthernet 1/0/1 で LLDP を無効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] undo lldp enable

関連コマンド

lldp global enable

5.1.9 lldp encapsulation snap

Syntax

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation snap**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **encapsulation**

デフォルト

LLDP フレームのカプセル化形式は Ethernet II です。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントのタイプを指定します。Ethernet interface view でエージェント タイプを指定しない場合、コマンドは nearest bridge エージェントの LLDP フレーム カプセル化形式を設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

nearest-nontpmr: nearest non-TPMR bridge エージェントを指定します。

説明

lldp encapsulation snap コマンドは、LLDP フレームのカプセル化形式を SNAP に設定します。

undo lldp encapsulation コマンドはデフォルトに戻します。

LLDP-CDP パケットは SNAP カプセル化のみを使用します。

例

GigabitEthernet 1/0/1 の LLDP フレームのカプセル化形式を SNAP に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] lldp encapsulation snap

5.1.10 lldp fast-count

Syntax

lldp fast-count *count*

undo lldp fast-count

デフォルト

高速LLDP フレーム送信がトリガーされるたびに、4 つのLLDP フレームが送信されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

count: 新しい隣接装置が検出される際に連続して送信される LLDP フレームの数を指定します。設定範囲は 1～8 です。

説明

lldp fast-count コマンドは新しい隣接装置が検出される際に連続して送信される LLDP フレームの数を指定します。

undo lldp fast-count コマンドはデフォルトに戻します。

例

新しい隣接装置が検出される際に連続して送信される LLDP フレームの数を 5 に設定します。

<AP> system-view

[AP] lldp fast-count 5

5.1.11 lldp global enable

Syntax

lldp global enable

undo lldp global enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

lldp global enable コマンドはグローバルで LLDP を有効にします。

undo lldp global enable コマンドはグローバルで LLDP を無効にします。

LLDP はグローバルとポートの両方で有効にしたときのみ適用されます。

例

グローバルで LLDP を無効にします。

<AP> system-view

[AP] undo lldp global enable

関連コマンド

lldp enable

5.1.12 lldp hold-multiplier

Syntax

lldp hold-multiplier *value*

undo lldp hold-multiplier

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

value: TTL の乗数を設定します。設定範囲は 2～10 です。

説明

lldp hold-multiplier コマンドは TTL の乗数を設定します。

undo lldp hold-multiplier コマンドはデフォルトに戻します。

LLDPDU で送信される TTL TLV は、受信装置で保存される装置情報の保存期間を決定します。

TTL の乗数を設定することにより、隣接装置に送信する TTL の設定を行うことができます。隣接装置についての情報の TTL は以下の式によって定義されます。

TTL ＝min（65535, （TTL の乗数 x LLDP フレームの送信間隔 ＋ 1））

TTL は最大 65535 秒です。65535 より大きい場合、65535 秒に丸められます。

例

TTL の乗数を 6 に設定します。

<AP> system-view

[AP] lldp hold-multiplier 6

関連コマンド

lldp timer tx-interval

5.1.13 lldp management-address-format string

Syntax

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **management-address-format string**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **management-address-format**

デフォルト

管理アドレスのエンコード形式は数値（numeric）です。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントのタイプを指定します。Ethernet interface view でエージェント タイプを指定しない場合、コマンドは nearest bridge エージェントの管理アドレスのエンコード形式を設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

nearest-nontpmr: nearest non-TPMR bridge エージェントを指定します。

説明

lldp Management-address-format string コマンドは、管理アドレスのエンコード形式を string に設定します。

undo lldp Management-address-format コマンドはデフォルトに戻します。

LLDP neighbors は、管理アドレスに同じエンコード形式を使用する必要があります。

neighbor がその管理アドレスを文字列形式でエンコードする場合は、接続ポートで management address のエンコード形式を文字列に設定します。

これにより、neighbor との正常な通信が保証されます。

例

GigabitEthernet 1/0/1 上の nearest customer bridge エージェントの management address のエンコード形式を文字列（string）に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] lldp agent nearest-customer management-address-format String

5.1.14 lldp notification remote-change enable

Syntax

lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable**

undo lldp [**agent** { **nearest-customer** | **nearest-nontpmr** }] **notification remote-change enable**

デフォルト

LLDP のトラップは、無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントのタイプを指定します。Ethernet interface view でエージェント タイプを指定しない場合、このコマンドは nearest bridge エージェントの LLDP トラップを有効にします。

nearest-customer: nearest customer bridge エージェントを指定します。

nearest-nontpmr: nearest non-TPMR bridge エージェントを指定します。

説明

lldp notification remote-change enable コマンドは LLDP トラップを有効にします。

undo lldp notification remote-change enable コマンドは LLDP トラップを無効にします。

ネットワークの初期段階では、ネットワーク トポロジは頻繁に変更されます。

このコマンドを使用すると、デバイスはトラップ情報をネットワーク管理システムに頻繁に送信するため、システムの負荷が増大し、リソースが浪費されます。

ベスト プラクティスとして、ネットワークの初期段階では LLDP トラップを有効にしないでください。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントの LLDP トラップを有効にします。

<AP> system-view

[AP] interface GigabitEthernet 1/0/1

[AP-GigabitEthernet1/0/1] lldp agent nearest-customer notification remote-change enable

5.1.15 lldp timer notification-interval

Syntax

lldp timer notification-interval *interval*

undo lldp timer notification-interval

デフォルト

30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: LLDP トラップと LLDP-MED トラップの送信間隔を指定します。設定範囲は 5 ～3600 秒です。

説明

lldp timer notification-interval コマンドはLLDP トラップと LLDP-MED トラップの送信間隔を設定します。

undo lldp timer notification-interval コマンドはデフォルトに戻します。

例

LLDP トラップと LLDP-MED トラップの送信間隔を 8 秒に設定します。

<AP> system-view

[AP] lldp timer notification-interval 8

5.1.16 lldp timer reinit-delay

Syntax

lldp timer reinit-delay *delay*

undo lldp timer reinit-delay

デフォルト

2 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

delay: LLDP の再初期化の遅延時間を設定します。設定範囲は 1～10 秒です。

説明

lldp timer reinit-delay コマンドは LLDP の再初期化の遅延時間を設定します。

undo lldp timer reinit-delay コマンドはデフォルトに戻します。

例

LLDP の再初期化の遅延時間を 4 秒に設定します。

<AP> system-view

[AP] lldp timer reinit-delay 4

5.1.17 lldp timer tx-interval

Syntax

lldp timer tx-interval *interval*

undo lldp timer tx-interval

デフォルト

30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: LLDP フレームの送信間隔を設定します。設定範囲は 5～32768 秒です。

説明

lldp timer tx-interval コマンドは LLDP フレームの送信間隔を設定します。

undo lldp timer tx-interval コマンドはデフォルトに戻します。

例

LLDP フレームの送信間隔を 20 秒に設定します。

<AP> system-view

[AP] lldp timer tx-interval 20

5.1.18 lldp tlv-enable

Syntax

- nearest bridge エージェント:

lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [*ip-address* **] } | dot1-tlv { all | port-vlan-id | protocol-vlan-id [** *vlan-id* **] | vlan-name [** *vlan-id* **] | management-vid [** *mvlan-id* **] } | dot3-tlv { all | mac-physic | max-frame-size | power | eee } | med-tlv { all | capability | inventory | network-policy [** *vlan-id* **] | power-over-ethernet | location-id { civic-address** *device-type country-code* **{** *ca-type ca-value* **}**&<1-10> **| elin-address** *tel-number* **} } }**

undo lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [*ip-address* **] } | dot1-tlv { all | port-vlan-id | protocol-vlan-id | vlan-name | management-vid } | dot3-tlv { all | mac-physic | max-frame-size | power | eee } | med-tlv { all | capability | inventory | network-policy [** *vlan-id* **] | power-over-ethernet | location-id } }**

- nearest non-TPMR bridge エージェント:

lldp agent nearest-nontpmr tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [*ip-address* **] } | dot1-tlv { all | port-vlan-id } }**

lldp tlv-enable dot1-tlv { protocol-vlan-id [*vlan-id* **] | vlan-name [** *vlan-id* **] | management-vid [** *mvlan-id* **] }**

undo lldp agent nearest-nontpmr tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [*ip-address*] } | dot1-tlv { all | port-vlan-id } }

undo lldp tlv-enable dot1-tlv { protocol-vlan-id | vlan-name | management-vid }

- For nearest customer bridge エージェント:

lldp agent nearest-customer tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [*ip-address*] } | dot1-tlv { all | port-vlan-id } } lldp tlv-enable dot1-tlv { protocol-vlan-id [*vlan-id*] | vlan-name [*vlan-id*] | management-vid [*mvlan-id*] }

undo lldp agent nearest-customer tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name | management-address-tlv [*ip-address*] } | dot1-tlv { all | port-vlan-id } }

undo lldp tlv-enable dot1-tlv { protocol-vlan-id | vlan-name | management-vid }

デフォルト

Layer 2 Ethernet インタフェースの場合:

- Nearest bridge エージェントは、次のタイプを除くすべてのタイプの LLDP TLV をアドバタイズできます。
  - 位置識別 TLV。
  - ポートとプロトコルの VLAN ID TLV。
  - VLAN 名 TLV。
  - 管理 VLAN ID TLV。
  - Energy-Efficient Ethernet TLV。
- Nearest non-TPMR bridge エージェントは TLV をアドバタイズしません。
- Nearest customer bridge エージェントは、basic TLVs および IEEE 802.1 organizationally specific TLVs をアドバタイズできます。

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

agent: LLDP エージェントのタイプを指定します。Ethernet interface view でエージェント タイプを指定しない場合、コマンドは nearest bridge エージェントのアドバタイズ可能な TLV のタイプを設定します。

nearest-customer: nearest customer bridge エージェントを指定します。

nearest-nontpmr: nearest non-TPMR bridge エージェントを指定します。

all: 指定されたタイプのすべての TLV をアドバタイズします。このキーワードにより、インタフェースは次の TLV をアドバタイズできるようになります。

- basic-tlv に all キーワードが指定されている場合。すべての basic LLDP TLV。
- dot1-tlv に all キーワードが指定されている場合。すべての IEEE 802.1 organizationally specific LLDP TLV。
- dot3-tlv に all キーワードが指定されている場合。すべての IEEE 802.3 organizationally specific LLDP TLV。
- すべてのキーワードが med-tlv に指定されている場合。位置識別 TLV を除くすべての LLDP-MED TLV。

basic-tlv: basic LLDP TLV をアドバタイズします。

management-address-tlv [ip-address | **interface loopback** *interface-number*]:

management address TLV をアドバタイズします。

interface loopback interface-number オプションは、番号で指定されたループバック インタフェースの IP アドレスとして management address を指定します。デフォルトでは、次のルールが適用されます。

lldp tlv-enable コマンド実行時：

以下の要件を満たす VLAN インタフェースの IPv4 アドレスが管理アドレスとしてアドバタイズされます。

- アップ状態。
- 対応する VLAN ID は、インタフェースで許可されている VLAN の中で最も小さいものです。
- 許可された VLAN のどの VLAN インタフェースにも IPv4 アドレスが割り当てられていない場合、またはすべての VLAN インタフェースがダウンしている場合は、インタフェースの MAC アドレスがアドバタイズされます。

undo lldp tlv-enable コマンド実行時：

- ip-address、またはインタフェース ループバック インタフェース番号を指定しない場合、インタフェースは管理アドレス TLV をアドバタイズしません。
- ip-address、またはインタフェース ループバック インタフェース番号を指定すると、インタフェースはデフォルトの管理アドレス TLV をアドバタイズします。

port-description: port description TLV をアドバタイズします。

system-capability: system capabilities TLV をアドバタイズします。

system-description: system description TLV をアドバタイズします。

system-name: system name TLV をアドバタイズします。

dot1-tlv: IEEE 802.1 organizationally specific LLDP TLV をアドバタイズします。

port-vlan-id: port VLAN ID TLV をアドバタイズします。

protocol-vlan-id [*vlan-id*]:

ポートとプロトコルの VLAN ID TLV をアドバタイズします。

vlan-id 引数は、アドバタイズされる TLV 内の VLAN ID を指定します。

VLAN ID の範囲は 1 ～ 4094 で、デフォルトはポート上の最小の VLAN ID です。

vlan-name [*vlan-id*]:

VLAN 名 TLV をアドバタイズします。

vlan-id 引数は、アドバタイズされる TLV 内の VLAN ID を指定します。

VLAN ID の範囲は 1 ～ 4094 で、デフォルトはポート上の最小の VLAN ID です。

VLAN ID を指定せず、ポートがどの VLAN にも割り当てられていない場合は、ポートの PVID がアドバタイズされます。

management-vid [*mvlan-id*]:

management VLAN ID TLV をアドバタイズします。

mvlan-id 引数は、アドバタイズされる TLV 内の管理 VLAN ID を指定します。

management VLAN ID の範囲は 1 ～ 4094 です。

このオプションを指定しない場合、値 0 がアドバタイズされます。これは、LLDP エージェントが management VLAN ID で構成されていないことを意味します。

dot3-tlv: IEEE 802.3 organizationally specific LLDP TLV をアドバタイズします。

mac-physic: MAC/PHY configuration/status TLV をアドバタイズします。

max-frame-size: maximum frame size TLV をアドバタイズします。

power: power in MDI TLV および power stateful control TLV をアドバタイズします。

eee: Energy-Efficient Ethernet TLV をアドバタイズします。

med-tlv: LLDP-MED TLV をアドバタイズします。

capability: LLDP-MED capabilities TLV をアドバタイズします。

inventory: 次の TLV をアドバタイズします。

hardware revision/firmware revision/software revision/serial number/manufacturer name/model name/and asset ID.

location-id: location identification TLV をアドバタイズします。

civic-address:

ネットワーク デバイスに関する一般的なアドレス情報を location identification TLV に挿入します。

device-type: デバイス タイプの値を 0 ～ 2 の範囲で設定します。

- 値 0 は DHCP サーバーを指定します。
- 値 1 はネットワーク デバイスを指定します。
- 値 2 は、LLDP-MED エンドポイントを指定します。

country-code: ISO 3166 で定義されている国コードを設定します。

{ *ca-type ca-value* }&<1-10>:

アドレス情報を設定します。

「*ca-type*」はアドレス情報の種類を 0～255 の範囲で表します。

「*ca-value*」はアドレス情報を表し、1～250 文字の文字列です。

「&<1-10>」は、最大 10 個の *ca-type ca-value* ペアを指定できることを示します。

elin-address: location identification TLV に緊急用の電話番号を挿入します。

tel-number : 緊急時の電話番号を 10～25 文字の文字列で設定します。

network-policy [*vlan-id*]:

network policy TLV をアドバタイズします。 vlan-id 引数は、アドバタイズする音声 VLAN ID を 1 ～ 4094 の範囲で指定します。

power-over-ethernet: 拡張された power-via-MDI TLV をアドバタイズします。

説明

lldp tlv-enable コマンドは、ポート上でアドバタイズ可能な TLV のタイプを設定します。

undo lldp tlv-enable コマンドは、ポート上の指定されたタイプの TLV のアドバタイズを無効にします。

すべてのキーワードを指定せずにこのコマンドを使用すると、デバイスが複数のタイプの TLV をアドバタイズできるようになります。

MAC/PHY configuration/status TLV がアドバタイズ可能でない場合、アドバタイズ可能かどうかに関係なく、LLDP-MED TLV はいずれもアドバタイズされません。

LLDP-MED capabilities TLV がアドバタイズできない場合、他の LLDP-MED TLV は、アドバタイズ可能かどうかに関係なくアドバタイズされません。

IEEE 802.1 organizationally specific LLDP TLV のポートおよびプロトコル VLAN ID、VLAN 名、および管理 VLAN ID TLV は、nearest bridge エージェントに対してのみ設定できます。

この設定は、nearest customer bridge エージェントおよび nearest non-TPMR bridge エージェントによって継承できます。

例

GigabitEthernet 1/0/1 の nearest customer bridge エージェントが、IEEE 802.1 organizationally specific TLV をアドバタイズできるようにします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] lldp agent nearest-customer tlv-enable dot1-tlv

目次

このセクションのページは **4-x-x** です。

6 章 レイヤ 2 フォワーディング 6-1
6.1 標準レイヤ 2 フォワーディング設定コマンド 6-1
6.1.1 display mac-forwarding statistics 6-1
6.1.2 reset mac-forwarding statistics 6-5

6章 レイヤ 2 フォワーディング

6.1 標準レイヤ2フォワーディング設定コマンド

6.1.1 display mac-forwarding statistics

Syntax

display mac-forwarding statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 種別と数字でインタフェースを指定します。本オプションを指定しない場合、コマンドは全インタフェースのフォワーディング統計情報を表示します。

説明

display mac-forwarding statistics コマンドはレイヤ 2 フォワーディング統計情報を表示します。

例

全インタフェースのレイヤ 2 フォワーディング統計情報を表示します。

<AP> display mac-forwarding statistics

```
Input:
  Sum:             888       Unknown Unicast:   0
  Broadcast:        0         Multicast:        0
  Filtered:         0         STP discarded:    0
  Service dropped:  0          Source dropped:   0
  Unknown dropped:  0          Learning dropped: 0
  Attack dropped:   0          Suppress dropped: 0
Deliver:
  Sum:             111       L2 protocol:      11
  Local MAC address: 100
Output:
  Sum:             666       Filtered:         0
```

```
  Blackhole dropped: 0          STP discarded:     0
  Service dropped:   0          Dest MAC dropped:  0
```

GigabitEthernet 1/0/1 インタフェースのレイヤ 2 フォワーディング統計情報を表示します。

<AP> display mac-forwarding statistics interface gigabitethernet 1/0/1

```
GigabitEthernet 1/0/1:
Input frames: 100    Output frames:100
Filtered:     0
```

表 6-1 コマンド出力

フィールド	説明
Input	インバウンドイーサネットフレームの統計情報 • **Sum**—受信したイーサネットフレームの総数。 • **Filtered**—802.1Q VLAN インバウンドフィルタリングルールによってフィルタリングされたイーサネットフレームの数。 • **STP discarded**— STP でブロックされたポートにおける破棄されたインバウンドイーサネットフレームの数。 • **Service dropped**—インバウンドサービス機能によって破棄されたイーサネットフレームの数。 • **Source dropped**—インバウンドサービス機能によって破棄されたイーサネットフレームの数。 • **Unknown dropped**—不明な送信元 MAC アドレスのフレームのフォワーディングが装置で無効になっているために破棄されたイーサネットフレームの数。 • **Learning dropped**— MAC アドレス学習数が上限に達した後に、不明な送信元 MAC アドレスのフレームのフォワーディングが装置で無効になっているために破棄されたイーサネットフレームの数。 • **Suppress dropped**—ストーム抑制によってドロップされたイーサネットフレームの数。 • **Broadcast**—受信したブロードキャストイーサネットフレームの数。 • **Multicast**—受信したマルチキャストイーサネットフレームの数。 • **Unknown Unicast**—受信した不明なユニキャストイーサネットフレームの数。 • **Blackhole dropped**—ブラックホール MAC アドレス宛てのために破棄されたイーサネットフレームの数。 • **Source MAC dropped**—送信元 MAC アドレスに基づく機能によってドロップされたイーサネットフレームの数。

フィールド	説明
Deliver	CPUに送出したイーサネットフレームの統計情報 • **Sum**— CPU に送出したイーサネットフレームの総数。 • **L2 protocol**— CPU に送出したレイヤ 2 プロトコルイーサネットフレームの数。 • **Local MAC address**—宛先 MAC アドレスがローカルレイヤ3 VLAN インタフェースの MAC アドレスであるイーサネットフレームの数。
Output	アウトバウンドイーサネットフレームの統計情報 • **Sum**— 送信されたイーサネットフレームの合計数。 • **Filtered**— 802.1Q VLAN アウトバウンドフィルタリングルールによってフィルタリングされたイーサネットフレームの数。 • **Blackhole dropped**—ブラックホール MAC アドレス宛てのために破棄されたイーサネットフレームの数。 • **STP discarded**— STP でブロックされたポートにおける破棄されたアウトバウンドイーサネットフレームの数。 • **Service dropped**—アウトバウンドサービス機能によって破棄されたイーサネットフレームの数。 • **Dest MAC dropped**—宛先 MAC アドレスに基づいて機能によって破棄されたイーサネットフレームの数。
GigabitEthernet1/0/1	GigabitEthernet 1/0/1のレイヤ2転送統計 • **Input frames**— ンタフェースで受信されたイーサネットフレームの数。 • **Output frames**— インタフェースで送信したイーサネットフレームの数。 • **Filtered**—他 VLAN からのものであるためにフィルタリングされたイーサネットフレームの数。

6.1.2 reset mac-forwarding statistics

Syntax

reset mac-forwarding statistics

View

User view

定義済みユーザロール

network-admin

network-operator

説明

reset mac-forwarding statistics コマンドはレイヤ 2 フォワーディング統計情報をクリアします。

例

レイヤ 2 フォワーディング統計情報をクリアします。

<AP> reset mac-forwarding statistics

目次

このセクションのページは **4-x-x** です。

7 章 ARP 7-1
7.1 ARP 設定コマンド 7-1
7.1.1 arp check enable 7-1
7.1.2 arp check log enable 7-2
7.1.3 arp max-learning-num 7-3
7.1.4 arp static 7-4
7.1.5 arp timer aging 7-6
7.1.6 display arp 7-7
7.1.7 display arp *ip-address* 7-9
7.1.8 display arp timer aging 7-10
7.1.9 reset arp 7-11
7.2 Gratuitous ARP 設定コマンド 7-12
7.2.1 arp ip-conflict log prompt 7-12
7.2.2 arp send-gratuitous-arp 7-13
7.2.3 gratuitous-arp-learning enable 7-14
7.2.4 gratuitous-arp-sending enable 7-16
7.3 Proxy ARP 設定コマンド 7-17
7.3.1 display local-proxy-arp 7-17
7.3.2 display proxy-arp 7-18
7.3.3 local-proxy-arp enable 7-19
7.3.4 proxy-arp enable 7-21

7章 ARP

7.1 ARP設定コマンド

7.1.1 arp check enable

Syntax

arp check enable

undo arp check enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

arp check enable コマンドはダイナミック ARP エントリチェックを有効にします。

undo arp check enable コマンドはダイナミック ARP エントリチェックを無効にします。

ダイナミック ARP エントリチェック機能は、マルチキャスト MAC アドレスを含むダイナミック ARP エントリのサポート状態にある装置を無効にします。その装置は、マルチキャストMACアドレスを含むダイナミックARPエントリを学習することができません。マルチキャスト MAC アドレスを含むスタティック ARP エントリを手動で追加する事は出来ません。

ダイナミック ARP エントリチェック機能が無効の場合、マルチキャスト MAC アドレスを含む ARP エントリがサポートされます。その装置は、ユニキャスト MAC アドレスをソースとする ARP パケットより供給されるマルチキャスト MAC アドレスを含むダイナミック ARP エントリを学習できます。また、マルチキャスト MAC アドレスを含むスタティック ARP エントリを手動で追加できます。

例

ダイナミック ARP エントリチェックを有効にします。

<AP> system-view

[AP] arp check enable

7.1.2 arp check log enable

Syntax

arp check log enable

undo arp check log enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp check log enable コマンドは ARP ロギング機能を有効にします。

undo arp check log enable コマンドは ARP ロギング機能を無効にします。

ARP が IP アドレスを正常に解決できないとき､装置で ARP イベントをロギングします。以下の ARP イベントをロギングできます。

- インタフェースで proxy ARP が無効な場合、受信した ARP パケットの宛先 IP アドレスが、受信インタフェースの IP アドレス、あるいは NAT 後のパブリック IP アドレスのいずれでもない時。
- 受信した ARP エントリの送信元 IP アドレスが、受信インタフェースの IP アドレス、あるいは NAT 後のパブリック IP アドレスと重複している時。

装置は Information Center に ARP ログメッセージを送信します。Information Center のログ出力ルールを設定するため､**info-center source** コマンドを使用します。Information Center の詳細はセクション 2 *システム管理 "Information Center"* を参照してください。

装置は非常に多くの ARP ログを作成することができます。システムリソースを保護するため、ARP イベントの調査、トラブルシューティングを行っているときのみ、ARP ロギング機能を有効にしてください。

例

ARP ロギング機能を有効にします。

<AP> system-view

[AP] arp check log enable

7.1.3 arp max-learning-num

Syntax

arp max-learning-num *max-number*

undo arp max-learning-num

デフォルト

816

View

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

max-number: インタフェースが学習できるダイナミック ARP エントリの最大数を指定します。設定範囲は 0～816 です。

説明

arp max-learning-num コマンドはインタフェースが学習できるダイナミック ARP エントリの最大数を設定します。

undo arp max-learning-num コマンドはデフォルトに戻します。

多くの ARP エントリを保持することを防ぐため、インタフェースが学習できるダイナミック ARP エントリの最大数を設定することができます。設定した最大数に到達すると、インタフェースは ARP エントリの学習を停止します。

0 に設定した場合、ダイナミック ARP エントリの学習を無効にします。

例

VLAN インタフェース 40 が学習できるダイナミック ARP エントリの最大数を 10 に設定します。

<AP> system-view

[AP] interface vlan-interface 40

[AP-Vlan-interface40] arp max-learning-num 10

GigabitEthernet 1/0/1 が学習できるダイナミック ARP エントリの最大数を 10 に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] arp max-learning-num 10

Bridge-aggregation 1 が学習できるダイナミック ARP エントリの最大数を 10 に設定します。

<AP> system-view

[AP] interface bridge-aggregation 1

[AP-Bridge-Aggregation1] arp max-learning-num 10

7.1.4 arp static

Syntax

arp static *ip-address mac-address* [*vlan-id interface-type interface-number*]
[**description** *text*]

undo arp *ip-address*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: スタティック ARP エントリの IP アドレスを指定します。

mac-address: スタティック ARP エントリの MAC アドレスを指定します。形式は H-H-H です。

vlan-id: ARP エントリが所属する VLAN の ID を指定します。設定範囲は 1～4094 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

description *text*: スタティック ARP エントリの説明を指定します。設定範囲は 1～255 です。大文字、小文字を区別します。

説明

arp static コマンドはスタティック ARP エントリを設定します。

undo arp コマンドはスタティック ARP エントリを削除します。

スタティック ARP エントリは手動で設定し維持します。スタティック ARP エントリはエージアウトしません。またダイナミック ARP エントリに上書きされることはありません。

スタティック ARP エントリはロングスタティック ARP エントリとショートスタティック ARP エントリに分類されます。

解決済みのショートスタティック ARP エントリは特定のイベントで未解決になります。たとえば、出力インタフェースがダウンしたとき、あるいは対応する VLAN や VLAN インタフェースが削除されたとき、未解決になります。

ロングスタティック ARP エントリは解決の場合と未解決の場合に分類されます。未解決のロングスタティック ARP エントリの場合、パケットの転送は行われません。ロングスタティック ARP エントリは以下の状態で未解決となり、パケットの転送に使用することができません。

- 対応する VLAN インタフェースあるいは出力インタフェースがダウンしている時。
- エントリの IP アドレスがローカル IP アドレスと競合している時。
- ローカルインタフェースに、ARP エントリの IP アドレスと同一のサブネットの IP アドレスがない時。

vlan-id interface-type interface-number を指定した場合、以下の制限とガイドラインに従ってください。

- インタフェースは Ethernet インタフェースまたは aggregate インタフェースを使用できます。
- VLAN、VLAN インタフェースはすでに作成されている必要があります。Ethernet インタフェースは VLAN に属している必要があります。
- VLAN インタフェースの IP アドレスと *ip-address* パラメータで指定された IP アドレスは同一ネットワークにする必要があります。
- VLAN あるいは VLAN インタフェースが削除された場合、VLAN のロングスタティック ARP エントリは削除されます。

例

IP アドレス 202.38.10.2、MAC アドレス 0000-fc01-0000、VLAN 10 の出力インタフェース GigabitEthernet 1/0/1 に対応するロングスタティック ARP エントリを設定します。

<AP> system-view

[AP] arp static 202.38.10.2 0000-fc01-0000 10 gigabitethernet 1/0/1

関連コマンド

- **display arp**
- **reset arp**

7.1.5 arp timer aging

Syntax

arp timer aging *aging-time*

undo arp timer aging

デフォルト

20 分

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: ダイナミック ARP エントリのエージングタイマを設定します。設定範囲は 1～1440 分です。

説明

arp timer aging コマンドはダイナミック ARP エントリのエージングタイマを設定します。

undo arp timer aging コマンドはデフォルトに戻します。

ARP テーブル上の各ダイナミック ARP エントリは有効期限を持っています。有効期限はエージングタイマと呼ばれ、有効期限内にダイナミック ARP エントリがアップデートされるたびに、エージングタイマはリセットされます。有効期限切れになる前に更新されなかったダイナミック ARP エントリは、ARP テーブルから削除されます。

必要に応じてダイナミック ARP エントリのエージングタイマを設定してください。たとえば proxy ARP を設定するとき、不正なダイナミック ARP エントリが時間内に削除されるようにエージングタイマを短い値に設定してください。

例

ダイナミック ARP エントリのエージングタイマを 10 分に設定します。

<AP> system-view

[AP] arp timer aging 10

関連コマンド

display arp timer aging

7.1.6 display arp

Syntax

display arp [[**all** | **dynamic** | **static**] | **vlan** *vlan-id* | **interface** *interface-type interface-number*] [**count** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての ARP エントリを表示します。

dynamic: ダイナミック ARP エントリを表示します。

static: スタティック ARP エントリを表示します。

vlan *vlan-id*: 指定した VLAN の ARP エントリを表示します。設定範囲は 1～4094 です。

interface *interface-type interface-number*: *interface-type interface-number* で指定されたインタフェースの ARP エントリを表示します。

count: ARP エントリ数を表示します。

verbose: ARP エントリの詳細情報を表示します。

説明

display arp コマンドは ARP エントリを表示します。

このコマンドは IP アドレス、MAC アドレス、VLAN ID、出力インタフェース、エントリタイプ、エージングタイマを含む ARP エントリの情報を表示します。

パラメータを指定しない場合、すべての ARP エントリを表示します。

例

すべての ARP エントリを表示します。

<AP> display arp all

```
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IP Address      MAC Address    VLAN/VSI name   Interface/Link ID  Aging Type
1.1.1.1         02e0-f102-0023     1           GE1/0/1             --    S
1.1.1.3         0000-fe50-6503    12           Tunnel1             15    D
1.1.1.4         000d-88f7-9f7d    12           0x1                 16    D
```

すべての ARP エントリの詳細情報を表示します。

<AP> display arp all verbose

```
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IP Address      : 1.1.1.1         SVID/CVID : 1          Aging   : --
MAC Address     : 02e0-f102-0023   Type: S          Nickname: 0x0000
Interface/Link ID: GE1/0/1
VPN Instance    : --
VSI Name        : --
VSI Interface   : --
...
```

すべての ARP エントリの数を表示します。

<AP> display arp all count

```
Total number of entries : 4
```

表 7-1 コマンド出力

フィールド	説明
IP Address	ARPエントリのIPアドレスです。
MAC Address	ARPエントリのMACアドレスです。
VLAN/VSI name	ARPエントリが所属するVSIのインデックス、あるいはVLANのIDです。以下のどちらかの状態である場合、**--**と表示されます。 ● ARPエントリが未解決のショートスタティックARPエントリです。 ● ARPエントリの出力インタフェースがVLANやVSIに所属していません。
Interface	ARPエントリの出力インタフェースです。ARPエントリが未解決のショートスタティックARPエントリである場合、**--**と表示されます。
Link ID	ARPエントリ内のリンクIDです。ARPエントリがどのVSIにも属していない場合、このフィールドにはハイフン(--)が表示されます。
Aging	ダイナミックARPエントリのエージングタイマです。単位は分です。**--**はエージングタイマが不明、あるいはエージングタイマが有効期限切れであることを示します。
Type	ARPエントリのタイプです。 ● **D**–ダイナミックARPエントリです。 ● **S**–スタティックARPエントリです。 ● **O**–オープンフロー。通常のソフトウェアでは未搭載。 ● **R**–ロール。 ● **I**–無効なARPエントリです。

フィールド	説明
SVLAN/CVLAN	ARPエントリが所属するCVLAN、あるいはSVLANのIDです。 以下のどちらかの状態である場合、--と表示されます。 • ARPエントリが未解決のショートスタティックARPエントリです。 • ARPエントリの出力インタフェースがSVLANやCVLANに所属していません。
NickName	ARPエントリのニックネームです。ニックネームは４ケタの16進数です。例えば、0x012a。
Description	ARPエントリの説明です。ARPエントリの説明が設定されていない場合は、このフィールドには--と表示されます。
Total number of entries	ARPエントリ数です。

関連コマンド

- **arp static**
- **reset arp**

7.1.7 display arp *ip-address*

Syntax

display arp *ip-address* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: 指定した IP アドレスの ARP エントリを表示します。

verbose: ARP エントリの詳細情報を表示します。

説明

display arp ip-address コマンドは IP アドレスの ARP エントリを表示します。

ARP エントリの情報は IP アドレス、MAC アドレス、VLAN ID、出力インタフェース、エントリタイプ、エージングタイマを含みます。

例

IP アドレス 20.1.1.1 の ARP エントリを表示します。

<AP> display arp 20.1.1.1

```
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IP Address      MAC Address    SVID    Interface     Aging Type
20.1.1.1        0000-fc00-0001   --         --          --   S
```

関連コマンド

- **arp static**
- **reset arp**

7.1.8 display arp timer aging

Syntax

display arp timer aging

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display arp timer aging コマンドはダイナミック ARP エントリのエージングタイマを表示します。

例

ダイナミック ARP エントリのエージングタイマを表示します。

<AP> display arp timer aging

```
Current ARP aging time is 10 minute(s)
```

関連コマンド

arp timer aging

7.1.9 reset arp

Syntax

reset arp { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべての ARP エントリを削除します。

dynamic: すべてのダイナミック ARP エントリを削除します。

static: すべてのスタティック ARP エントリを削除します。

interface *interface-type interface-number*: *interface-type interface-number* で指定されたインタフェースの ARP エントリを削除します。指定しない場合、すべてのインタフェースの ARP エントリを削除します。

説明

reset arp コマンドは ARP テーブルから ARP エントリを削除します。

例

すべてのスタティック ARP エントリを削除します。

<AP> reset arp static

関連コマンド

- **arp static**
- **display arp**

7.2 Gratuitous ARP設定コマンド

7.2.1 arp ip-conflict log prompt

Syntax

arp ip-conflict log prompt

undo arp ip-conflict log prompt

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

arp ip-conflict log prompt コマンドは IP 重複の通知を有効にします。

undo arp ip-conflict log prompt コマンドはデフォルトに戻します。

例

装置で IP 重複の通知を有効にします。

<AP> system-view

[AP] arp ip-conflict log prompt

7.2.2 arp send-gratuitous-arp

Syntax

arp send-gratuitous-arp [**interval** *interval*]

undo arp send-gratuitous-arp

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: gratuitous ARP パケットを送信する送信間隔を設定します。設定範囲は 200～200000 ミリ秒です。なお、ARP パケットを送信する送信間隔のデフォルト値は、2000 ミリ秒です。

説明

arp send-gratuitous-arp コマンドはインタフェースで gratuitous ARP パケットの定期送信を有効にし、送信間隔を設定します。

undo arp send-gratuitous-arp コマンドはインタフェースで gratuitous ARP パケットを定期的に送信することを無効にします。

このコマンドは有効にしたインタフェースのデータリンクレイヤの状態が up で、且つ IP アドレスが設定されているときのみ、適用されます。

この機能はインタフェースのプライマリ IP アドレス、あるいは手動で設定されたセカンダリ IP アドレスの gratuitous ARP 要求のみ送信することができます。プライマリ IP アドレスは手動または自動で設定することができますが、セカンダリ IP アドレスは手動で設定する必要があります。

gratuitous ARP パケットの送信間隔を変更すると、次の送信間隔から設定が適用されます。

gratuitous ARP パケットの送信間隔は以下の状況によって、設定した値よりも長くなります。

- 複数のインタフェースで有効にされた場合
- 各インタフェースで複数のセカンダリ IP アドレスが設定された場合
- 優先する状況で短い送信間隔を設定した場合

例

VLAN インタフェース 2 で gratuitous ARP パケットの定期送信を有効にし、送信間隔を 300 ミリ秒に設定します。

<AP> system-view

[AP] interface vlan-interface 2

[AP-Vlan-interface2] arp send-gratuitous-arp interval 300

7.2.3 gratuitous-arp-learning enable

Syntax

gratuitous-arp-learning enable

undo gratuitous-arp-learning enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-learning enable コマンドは gratuitous ARP パケットの学習機能を有効にします。

undo gratuitous-arp-learning enable コマンドは gratuitous ARP パケットの学習機能を無効にします。

gratuitous ARP パケットの学習機能は、装置が受信した gratuitous ARP パケットをもとに ARP エントリを作成あるいはアップデートすることで ARP テーブルを維持することができます。

学習機能が無効であるとき、装置は既存の ARP エントリのみをアップデートするため受信した gratuitous ARP パケットを使用します。ARP エントリは受信した gratuitous ARP パケットをもとに作成されません。これは ARP テーブルの空き容量を節約します。

例

gratuitous ARP パケットの学習機能を有効にします。

<AP> system-view

[AP] gratuitous-arp-learning enable

7.2.4 gratuitous-arp-sending enable

Syntax

gratuitous-arp-sending enable

undo gratuitous-arp-sending enable

デフォルト

デバイスは、送信者の IP アドレスが異なるサブネット上にある ARP 要求を受信した場合、Gratuitous ARP パケットを送信しません。

View

System view

定義済みユーザロール

network-admin

説明

gratuitous-arp-sending enable コマンドは異なるサブネットから ARP 要求を受信した際に、gratuitous ARP パケットの送信を有効にします。

undo gratuitous-arp-sending enable コマンドはデフォルトに戻します。

例

異なるサブネットから ARP 要求を受信した際に、gratuitous ARP パケットの送信を無効にします。

<AP> system-view

[AP] undo gratuitous-arp-sending enable

7.3 Proxy ARP設定コマンド

7.3.1 display local-proxy-arp

Syntax

display local-proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースのローカル Proxy ARP のタイプとナンバーを表示します。

説明

display local-proxy-arp コマンドはローカル Proxy ARP の状態を表示します。

ローカル Proxy ARP の状態は有効あるいは無効にすることができます。

インタフェースを指定した場合、指定したインタフェースのローカル Proxy ARP の状態を表示します。

インタフェースを指定しない場合、すべてのインタフェースのローカル Proxy ARP の状態を表示します。

例

VLAN インタフェース 2 のローカル Proxy ARP の状態を表示します。

<AP> display local-proxy-arp interface vlan-interface 2

```
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

関連コマンド

local-proxy-arp enable

7.3.2 display proxy-arp

Syntax

display proxy-arp [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースの Proxy ARP のタイプとナンバーを表示します。

説明

display proxy-arp コマンドは Proxy ARP の状態を表示します。

Proxy ARP の状態は有効あるいは無効にすることができます。

インタフェースを指定した場合、指定したインタフェースの Proxy ARP の状態を表示します。

インタフェースを指定しない場合、すべてのインタフェースの Proxy ARP の状態を表示します。

例

VLAN インタフェース 1 の Proxy ARP の状態を表示します。

<AP> display proxy-arp interface Vlan-interface 1

```
Interface Vlan-interface1
 Proxy ARP status: disabled
```

関連コマンド

proxy-arp enable

7.3.3 local-proxy-arp enable

Syntax

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

undo local-proxy-arp enable

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

パラメータ

ip-range *start-ip-address* **to** *end-ip-addrerss*: ローカル Proxy ARP を有効にする IP アドレスの範囲を指定します。*start-ip-address* は *end-ip-address* 以下の値にしてください。

説明

local-proxy-arp enable コマンドはローカル Proxy ARP を有効にします。

undo local-proxy-arp enable コマンドはローカル Proxy ARP を無効にします。

Proxy ARP は異なるネットワークの IP アドレスの ARP 要求に応答するため、ネットワークの装置で有効にします。Proxy ARP を有効にすることで、異なるブロードキャストドメインのホストが同一のブロードキャストドメインにいるように互いに通信できるようにします。

Proxy ARP は一般的な Proxy ARP とローカル Proxy ARP があります。

一般的な Proxy ARP は異なるレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ローカル Proxy ARP は同一のレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ip-range によって範囲の設定を複数実行した場合、最後に行った設定が適用されます。

例

VLAN インタフェース 2 でローカル Proxy ARP を有効にします。

<AP> system-view

[AP] interface vlan-interface 2

[AP-Vlan-interface2] local-proxy-arp enable

VLAN インタフェース 2 で IP アドレス範囲 1.1.1.1～1.1.1.20 のローカル Proxy ARP を有効にします。

<AP> system-view

[AP] interface vlan-interface 2

[AP-Vlan-interface2] local-proxy-arp enable ip-range 1.1.1.1 to 1.1.1.20

関連コマンド

display local-proxy-arp

7.3.4 proxy-arp enable

Syntax

proxy-arp enable

undo proxy-arp enable

デフォルト

無効

View

VLAN interface view

定義済みユーザロール

network-admin

説明

proxy-arp enable コマンドは Proxy ARP を有効にします。

undo proxy-arp enable コマンドは Proxy ARP を無効にします。

Proxy ARP は異なるネットワークの IP アドレスの ARP 要求に応答するため、ネットワークの装置で有効にします。Proxy ARP を有効にすることで、異なるブロードキャストドメインのホストが同一のブロードキャストドメインにいるように互いに通信できるようにします。

Proxy ARP は一般的な Proxy ARP とローカル Proxy ARP があります。

一般的な Proxy ARP は異なるレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

ローカル Proxy ARP は同一のレイヤ 3 インタフェースに接続され、異なるブロードキャストドメインに存在するホスト間で通信することができます。

例

VLAN インタフェース 2 で Proxy ARP を有効にします。

<AP> system-view

[AP] interface vlan-interface 2

[AP-Vlan-interface2] proxy-arp enable

関連コマンド

display proxy-arp

目次

このセクションのページは **4-x-x** です。

8 章 IP アドレス 8-1
8.1 IP アドレス設定コマンド 8-1
8.1.1 display ip interface 8-1
8.1.2 display ip interface brief 8-5
8.1.3 ip address 8-7

8章 IP アドレス

8.1 IPアドレス設定コマンド

8.1.1 display ip interface

Syntax

display ip interface [*interface-type* [*interface-number*]]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type: インタフェースを種別で指定します。

interface-number: インタフェースを番号で指定します。

説明

display ip interface コマンドは指定したレイヤ 3 インタフェースの IP の設定と統計情報を表示します。

統計情報には以下の情報が含まれます。

- ユニキャストパケットの数、バイト、インタフェースが送受信したマルチキャストパケットが含まれます。
- TTL 無効のパケットの数、インタフェースが受信した ICMP パケットの数が含まれます。

パケット統計情報は、ネットワークに対する攻撃の可能性を見つけるのに役立ちます。

インタフェースタイプのみを指定した場合、このインタフェースタイプのすべてのインタフェースの IP 設定と統計情報が表示されます。オプションのパラメータを指定しない場合、このコマンドはすべてのレイヤ 3 インタフェースの IP 設定と統計情報を表示します。

例

VLAN インタフェース 10 の IP の設定と統計情報を表示します。

<AP> display ip interface vlan-interface 10

```
Vlan-interface10 current state : DOWN
```

```
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
TTL invalid packet number:        0
ICMP packet input number:         0
  Echo reply:                    0
  Unreachable:                   0
  Source quench:                 0
  Routing redirect:              0
  Echo request:                  0
  Router advert:                 0
  Router solicit:                0
  Time exceed:                   0
  IP header bad:                 0
  Timestamp request:             0
  Timestamp reply:               0
  Information request:           0
  Information reply:             0
  Netmask request:               0
  Netmask reply:                 0
  Unknown type:                  0
```

表 8-1 コマンド出力

フィールド	説明
current state	インタフェースの現在の物理状態です。 • **Administrative DOWN**—インタフェースが**shutdown**コマンドでシャットダウンしています。 • **DOWN**—インタフェースが管理上upとなっていますが、物理的にdownしています。ケーブル接続あるいはリンク障害によって引き起こされる可能性があります。 • **UP**—インタフェースが管理上および物理的にupとなっています。
Line protocol current state	リンクレイヤプロトコルの現在の状態です。 • **DOWN**—インタフェースのプロトコル状態がdownしています。 • **UP**—インタフェースのプロトコル状態がupしています。 • **UP (spoofing)**—インタフェースのプロトコル状態がUpしているように見せかけていることを示します。対応するリンクが存在しない、あるいはリンクがオンデマンドで

フィールド	説明
	のみ設定されることを示します。
Internet address is ip-address/mask-length (Type)	インタフェースのIPアドレスです。 • **Primary**—プライマリIPアドレスです。 • **Sub**—セカンダリIPアドレスです。 • **DHCP-Allocated**—DHCPによって取得したIPアドレスです。 • **BOOTP-Allocated**—BOOTPによって取得したIPアドレスです。
Broadcast address	インタフェースに接続されたサブネットのブロードキャストアドレスです。
The Maximum Transmit Unit	インタフェースのMTU（最大転送ユニット）です。単位はバイトです。
input packets, bytes, multicasts output packets, bytes, multicasts	インタフェースで受信したユニキャストパケット、バイト、マルチキャストパケットです。（装置起動時に統計情報の取得が開始されます。）
TTL invalid packet number	インタフェースで受信したTTL無効のパケット数です。（装置起動時に統計情報の取得が開始されます。）
ICMP packet input number: Echo reply: Unreachable: Source quench: Routing redirect: Echo request: Router advert: Router solicit: Time exceed: IP header bad: Timestamp request: Timestamp reply: Information request: Information reply: Netmask request: Netmask reply: Unknown type:	インタフェースで受信したICMPパケットの総数です。（装置起動時に統計情報の取得が開始されます。） • **Echo reply packets**－エコー応答パケットです。 • **Unreachable packets**－到達不能パケットです。 • **Source quench packets**－送信元抑制パケットです。 • **Routing redirect packets**－ルーティングリダイレクトパケットです。 • **Echo request packets**－エコー要求パケットです。 • **Router advertisement packets**－ルータ通知パケットです。 • **Router solicitation packets**－ルータ選択要求パケットです。 • **Time exceeded packets**－時間超過パケットです。 • **IP header bad packets**－IPヘッダ不良パケットです。 • **Timestamp request packets**－タイムスタンプ要求パケットです。 • **Timestamp reply packets**－タイムスタンプ応答パケットです。 • **Information request packets**－情報要求パケットです。 • **Information reply packets**－情報応答パケットです。 • **Netmask request packets**－ネットマスク要求パケットです。 • **Netmask reply packets**－ネットマスク応答パケットです。

フィールド	説明
	• **Unknown type packets**－不明なタイプのパケットです。

関連コマンド

- **display ip interface brief**
- **ip address**

8.1.2 display ip interface brief

Syntax

display ip interface [*interface-type* [*interface-number*]] **brief** [**description**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type: インタフェースタイプを指定します。指定しない場合、すべてのレイヤ 3 インタフェースの IP 設定の概要情報を表示します。

interface-number: インタフェース番号を指定します。指定しない場合、指定したタイプのすべてのレイヤ 3 インタフェースの IP 設定の概要情報を表示します。

description: インタフェースの完全な説明を表示します。このキーワードを指定しない場合、インタフェースの説明ごとに最大 11 文字が表示されます。説明が 11 文字を超える場合は、最初の 8 文字が表示され、その後に省略記号 (...) が表示されます。

説明

display ip interface brief コマンドはレイヤ 3 インタフェースの IP 設定の概要情報を表示します。物理リンクの状態、リンクレイヤプロトコルの状態、IP アドレス、インタフェースの説明が含まれます。

例

VLAN インタフェースの IP 設定の概要情報を表示します。

<AP> display ip interface vlan-interface brief

```
*down: administratively down
(s): spoofing  (l): loopback
Interface          Physical Protocol IP address             Description
Vlan10             down     down     6.6.6.1        --       Link to Co...
```

表 8-2 コマンド出力

フィールド	説明
*down: administratively down	インタフェースが**shutdown**コマンドでシャットダウンしています。

フィールド	説明
(s) : spoofing	インタフェースのスプーフィング属性です。リンクレイヤプロトコルがUp表示されているインタフェースにリンクがない、あるいはリンクがオンデマンドでのみ設定されることを示します。
Interface	インタフェース名です。
Physical	インタフェースの物理状態です。 ● ***down**—インタフェースが**shutdown**コマンドでシャットダウンしています。 ● **down**—インタフェースが管理上upとなっていますが、物理的にdownしています。ケーブル接続あるいはリンク障害によって引き起こされる可能性があります。 ● **up**—インタフェースが管理上および物理的にupとなっています。
Protocol	インタフェースのリンクレイヤプロトコルの状態です。 ● **down**—インタフェースのプロトコル状態がdownしています。 ● **down(l)**—ループバックインタフェースのプロトコル状態がdownしています。 ● **up**—インタフェースのリンクレイヤプロトコルがupです。 ● **up(l)**—ループバックインタフェースのリンクレイヤプロトコルがupです。 ● **up(s)**—インタフェースのプロトコル状態がup（spoofing）です。
IP address/Mask	インタフェースのIPアドレスです。設定されていない場合、（--）と表示されます。
Description	インタフェースの説明の情報です。 説明が設定されていない場合、（--）と表示されます。

関連コマンド

- **display ip interface**
- **ip address**

8.1.3 ip address

Syntax

ip address *ip-address* { *mask-length* | *mask* } [**sub**]

undo ip address [*ip-address* { *mask-length* | *mask* } [**sub**]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: インタフェースの IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: サブネットマスクの長さを指定します。設定範囲は 1～31 です。ループバックインタフェースの設定範囲は 1～32 です。

mask: サブネットマスクを指定します。ドットで区切り、10 進数で指定します。

sub: インタフェースにセカンダリ IP アドレスを割り当てます。

説明

ip address コマンドはインタフェースに IP アドレスを割り当てます。

undo ip address コマンドはインタフェースから IP アドレスを削除します。

インタフェースのプライマリ IP アドレスあるいはセカンダリ IP アドレスを設定するために、このコマンドを使用します。

インタフェースは 1 つのプライマリ IP アドレスのみ設定することができます。新しく設定されたプライマリ IP アドレスは、古いアドレスを上書きします。インタフェースが複数のサブネットに接続されている場合、サブネットがインタフェースを通して通信できるように、プライマリ IP アドレスとサブネットを設定します。

BOOTP、DHCP、PPP を通して IP アドレスを取得するインタフェースはセカンダリ IP アドレスを設定することができません。

undo ip address コマンドはインタフェースからすべての IP アドレスを削除します。

undo ip address *ip-address* { *mask* | *mask-length* }コマンドはプライマリ IP アドレスを削除します。**undo ip address** *ip-address* { *mask* | *mask-length* } **sub** コマンドはセカンダリ IP アドレスを削除します。

インタフェースに割り当てたプライマリ IP アドレスとセカンダリ IP アドレスは同一ネットワークセグメント上に設定することができますが、装置の異なるインタフェースは異なるネットワークセグメント上に存在する必要があります。

例

VLAN インタフェース 10 にプライマリ IP アドレスを 129.12.0.1、セカンダリ IP アドレスを 202.38.160.1、サブネットマスクを 255.255.255.0 に設定します。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] ip address 129.12.0.1 255.255.255.0

[AP-Vlan-interface10] ip address 202.38.160.1 255.255.255.0 sub

関連コマンド

- **display ip interface**
- **display ip interface brief**

目次

このセクションのページは **4-x-x** です。

9 章 DHCP 9-1
9.1 DHCP 設定コマンド 9-1
9.1.1 dhcp dscp 9-1
9.1.2 dhcp enable 9-2
9.1.3 dhcp select 9-2
9.2 DHCP サーバ設定コマンド 9-4
9.2.1 address range 9-4
9.2.2 bims-server 9-6
9.2.3 bootfile-name 9-8
9.2.4 class option-group 9-9
9.2.5 dhcp class 9-10
9.2.6 dhcp option group 9-12
9.2.7 dhcp server apply ip-pool 9-13
9.2.8 dhcp server forbidden-ip 9-14
9.2.9 dhcp server ip-pool 9-16
9.2.10 dhcp server ping packets 9-17
9.2.11 dhcp server ping timeout 9-18
9.2.12 dhcp server relay information enable 9-19
9.2.13 display dhcp server conflict 9-19
9.2.14 display dhcp server expired 9-20
9.2.15 display dhcp server free-ip 9-22
9.2.16 display dhcp server ip-in-use 9-23
9.2.17 display dhcp server pool 9-26
9.2.18 display dhcp server statistics 9-30
9.2.19 dns-list 9-32
9.2.20 domain-name 9-33
9.2.21 expired 9-34
9.2.22 forbidden-ip 9-36
9.2.23 gateway-list 9-37
9.2.24 if-match 9-39
9.2.25 nbns-list 9-41
9.2.26 netbios-type 9-42
9.2.27 network 9-44
9.2.28 next-server 9-46
9.2.29 option 9-47
9.2.30 reset dhcp server conflict 9-49

9.2.31 reset dhcp server expired 9-50
9.2.32 reset dhcp server ip-in-use 9-51
9.2.33 reset dhcp server statistics 9-52
9.2.34 static-bind 9-53
9.2.35 tftp-server domain-name 9-55
9.2.36 tftp-server ip-address 9-56
9.2.37 voice-config 9-57
9.3 DHCP リレーエージェント設定コマンド 9-59
9.3.1 dhcp relay client-information record 9-59
9.3.2 dhcp relay client-information refresh enable 9-60
9.3.3 dhcp relay information circuit-id 9-61
9.3.4 dhcp relay information enable 9-63
9.3.5 dhcp relay information remote-id 9-65
9.3.6 dhcp relay information strategy 9-67
9.3.7 dhcp relay release ip 9-69
9.3.8 dhcp relay server-address 9-70
9.3.9 display dhcp relay client-information 9-71
9.3.10 display dhcp relay information 9-73
9.3.11 display dhcp relay server-address 9-75
9.3.12 display dhcp relay statistics 9-76
9.3.13 reset dhcp relay client-information 9-77
9.3.14 reset dhcp relay statistics 9-78
9.4 DHCP クライアント設定コマンド 9-79
9.4.1 dhcp client dad enable 9-79
9.4.2 dhcp client dscp 9-80
9.4.3 display dhcp client 9-80
9.4.4 ip address dhcp-alloc 9-84
9.5 BOOTP クライアント設定コマンド 9-85
9.5.1 display bootp client 9-85
9.5.2 ip address bootp-alloc 9-87

9章 DHCP

9.1 DHCP設定コマンド

9.1.1 dhcp dscp

Syntax

dhcp dscp *dscp-value*

undo dhcp dscp

デフォルト

56

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DHCP パケットの DSCP を設定します。設定範囲は 0～63 です。

説明

dhcp dscp コマンドは DHCP サーバあるいは DHCP リレーエージェントに送信される DHCP パケットの DSCP を設定します。

undo dhcp dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

DHCP パケットの DSCP を 30 に設定します。

<AP> system-view

[AP] dhcp dscp 30

9.1.2 dhcp enable

Syntax

dhcp enable

undo dhcp enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp enable コマンドは DHCP を有効にします。

undo dhcp enable コマンドは DHCP を無効にします。

DHCP に関する設定は DHCP を有効にしたのち適用されます。

DHCP サーバあるいは DHCP リレーエージェントの設定を実行する前に、DHCP を有効にしてください。

例

DHCP を有効にします。

<AP> system-view

[AP] dhcp enable

9.1.3 dhcp select

Syntax

dhcp select { **relay** | **server** }

undo dhcp select { **relay** | **server** }

デフォルト

インタフェースは DHCP サーバモードで動作し、設定パラメータの DHCP 要求に応答します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

relay: インタフェースで DHCP リレーエージェントを有効にします。

server: インタフェースで DHCP サーバを有効にします。

説明

dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを有効にします。

undo dhcp select コマンドはインタフェースで DHCP サーバあるいは DHCP リレーエージェントを無効にします。無効にした場合、インタフェースは受信した DHCP パケットを廃棄します。

インタフェースで DHCP サーバモードを DHCP リレーエージェントモードに変更する前に、**reset dhcp server ip-in-use** コマンドでアドレスの割り当てと許可された ARP エントリを削除してください。これらの割り当ては、DHCP リレーエージェントが有効になったのち、作成される ARP エントリと重複する可能性があります。

例

VLAN インタフェース 2 で DHCP リレーエージェントを有効にします。

<AP> system-view

[AP] interface vlan-interface 2

[AP-Vlan-interface2] dhcp select relay

9.2 DHCPサーバ設定コマンド

9.2.1 address range

Syntax

address range *start-ip-address end-ip-address*

undo address range

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 開始 IP アドレスを指定します。

end-ip-address: 終了 IP アドレスを指定します。

説明

address range コマンドはダイナミックの割り当てを行うため DHCP アドレスプールの IP アドレス範囲を設定します。

undo address range コマンドは DHCP アドレスプールの IP アドレス範囲を削除します。

IP アドレス範囲が指定されていない場合、address pool view で **network** コマンドを使用してサブネットのすべての IP アドレスを割り当てることができます。IP アドレス範囲が指定されている場合、IP アドレス範囲の IP アドレスのみを割り当てることができます。

address range コマンドを使用した後、アドレスプールのセカンダリサブネットを指定するため、**network secondary** コマンドを使用することができません。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

address range で指定されたアドレス範囲は **network** コマンドで指定されたサブネット内にある必要があります。範囲外のアドレスを割り当てることはできません。

例

アドレスプール 1 の 192.168.8.1～192.168.8.150 のアドレス範囲を指定します。

<AP> system-view

[AP] dhcp server ip-pool 1

[AP-dhcp-pool-1] address range 192.168.8.1 192.168.8.150

関連コマンド

- **display dhcp server pool**
- **network**

9.2.2 bims-server

Syntax

bims-server ip *ip-address* [**port** *port-number*] **sharekey** { **cipher** | **simple** } *string*

undo bims-server

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: BIMS サーバの IP アドレスを指定します。

port *port-number*: BIMS サーバのポート番号を指定します。設定範囲は 1～65534 です。
cipher: 暗号テキストキーを設定します。

simple: プレーンテキストキーを設定します。

string: キーの文字列を設定します。大文字小文字を区別します。**simple** を指定した場合、プレーンテキストで 1～16 の文字列でなくてはなりません。**cipher** を設定した場合、1～53 文字の暗号テキストでなければなりません。BIMS サーバに送られたパケットを暗号化するために DHCP クライアントは共有キーを使用します。

説明

bims-server コマンドは DHCP アドレスプールの BIMS サーバの IP アドレス、ポート番号、共有キーを指定します。

undo bims-server コマンドは指定された BIMS サーバ情報を削除します。

コマンドを複数回、設定した場合、最後に行った設定が適用されます。

セキュリティ目的のため、プレーンテキストで設定されたパスワードも含め、すべてのパスワードは暗号テキストで保存されます。

例

BIMS サーバの IP アドレス 1.1.1.1、ポート番号 80、共有キーaabbcc アドレスプール 0 に指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey simple aabbcc

関連コマンド

display dhcp server pool

9.2.3 bootfile-name

Syntax

bootfile-name *bootfile-name*

undo bootfile-name

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

bootfile-name: コンフィグレーションファイル名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

bootfile-name コマンドはコンフィグレーションファイル名を指定します。

undo bootfile-name コマンドはコンフィグレーションファイル名を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

コンフィグレーションファイルが TFTP サーバにある場合、TFTP サーバのコンフィグレーションファイル名を指定します。

例

DHCP アドレスプール 0 のブートファイル名 boot.cfg を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] bootfile-name boot.cfg

関連コマンド

- **display dhcp server pool**
- **next-server**
- **tftp-server domain-name**
- **tftp-server ip-address**

9.2.4 class option-group

Syntax

class *class-name* **option-group** *option-group-number*

undo class *class-name* **option-group**

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

class-name: DHCP ユーザクラスの名前を指定します。設定範囲は 1～63 文字で、大文字と小文字は区別しません。

option-group-number: DHCP オプショングループに 1 から 32768 までの番号を割り当てます。

説明

class option-group コマンドは DHCP ユーザクラスの DHCP オプショングループを指定します。

undo class option-group コマンドは DHCP ユーザクラスの DHCP オプショングループ設定を削除します。

DHCP-DISCOVER メッセージを受信すると、サーバはこのコマンドで指定された順序で DHCP クライアントと DHCP ユーザクラスを比較します。一致する DHCP ユーザクラスが見つかった場合、サーバはクライアントにオプショングループの DHCP オプションを割り当てます。複数の DHCP ユーザクラスと一致した場合、サーバは次のようにオプショングループを選択します。

· オプショングループに共通のオプションがある場合、サーバは最初に一致したユーザクラスに指定されたオプショングループを選択します。

· オプショングループのオプションが異なる場合、サーバは一致するオプショングループをすべて選択します。

DHCP アドレスプール内の DHCP ユーザクラスに指定できるオプショングループは 1 つだけです。ユーザクラスに対してこのコマンドを複数回実行すると、最新の設定が有効になります。

例

DHCP アドレスプール 0 の DHCP ユーザクラス user に、DHCP オプショングループ 1 を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] class user option-group 1

関連コマンド

dhcp option-group

9.2.5 dhcp class

Syntax

dhcp class *class-name*

undo dhcp class *class-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

class-name: DHCP ユーザクラスの名前を指定します。設定範囲は 1～63 文字で、大文字と小文字は区別しません。

説明

dhcp class コマンドは DHCP ユーザクラスを作成し、その view に移行します。

undo dhcp class コマンドは指定した DHCP ユーザクラスを削除します。

またコマンドを使用して既存の DHCP ユーザクラス View に移行することができます。

DHCP ユーザクラス View では、if-match コマンドを使用して、DHCP クライアントを DHCP ユーザクラスに紐付ける一致ルールを設定できます。

例

DHCP ユーザクラス test を作成し、その View に移行します。

<AP> system-view

[AP] dhcp class test

[AP-dhcp-class-test]

関連コマンド

- **class option-group**
- **if-match**

9.2.6 dhcp option group

Syntax

dhcp option-group *option-group-number*

undo dhcp option-group *option-group-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

option-group-number: DHCP オプショングループに 1 から 32768 までの番号を割り当てます。

説明

dhcp option group コマンドは DHCP オプショングループを作成し、その view に移行します。

undo dhcp option group コマンドは指定した DHCP オプショングループを削除します。

またコマンドを使用して既存の DHCP オプショングループ View に移行することができます。

例

DHCP オプショングループ 1 を作成し、その View に移行します。

<AP> system-view

[AP] dhcp option-group 1

[AP-dhcp-option-group-1]

関連コマンド

- **class option-group**
- **option**

9.2.7 dhcp server apply ip-pool

Syntax

dhcp server apply ip-pool *pool-name*

undo dhcp server apply ip-pool

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

pool-name: DHCP アドレスプールの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

dhcp server apply ip-pool コマンドはインタフェースにアドレスプールを適用します。

undo dhcp server apply ip-pool コマンドは設定を削除します。

インタフェースから DHCP 要求を受信すると、DHCP サーバはすべてのアドレスプールから、割り当て可能な DHCP クライアントの IP アドレスを検索します。

このコマンドが設定されている場合は、サーバはインタフェースに適用されたアドレスプールから、DHCP クライアントに IP アドレスを割り当てます。アドレスプールに割り当て可能な IP アドレスがない、または、アドレスプール自体が存在しない場合は、DHCP クライアントは IP アドレスを取得することができません。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

VLAN インタフェース 2 に DHCP アドレスプール 0 を適用します。

<AP> system-view

[AP] interface vlan-interface 2

[AP-Vlan-interface2] dhcp server apply ip-pool 0

関連コマンド

dhcp server ip-pool

9.2.8 dhcp server forbidden-ip

Syntax

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

undo dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

start-ip-address: 開始 IP アドレスを指定します。

end-ip-address: 終了 IP アドレスを指定します。*end-ip-address* は *start-ip-address* より小さい値にすることができません。指定されない場合、*start-ip-address* のみがダイナミック割り当てから除外されます。

説明

dhcp server forbidden-ip コマンドはダイナミック割り当てから指定した IP アドレスを除外します。

undo dhcp server forbidden-ip コマンドは設定を削除します。

ゲートウェイと FTP サーバのような装置の IP アドレスはクライアントに割り当てることができません。このコマンドはダイナミック割り当てからそのようなアドレスを除外します。

除外された IP アドレスがスタティックの割り当てにある場合、クライアントに割り当てることができます。

undo dhcp server forbidden-ip コマンドでアドレスあるいはアドレス範囲を削除する場合、**dhcp server forbidden-ip** コマンドで指定したアドレスあるいはアドレス範囲と同一にしてください。

アドレス範囲の一部の IP アドレスを削除する場合、アドレス範囲全体を削除する必要があります。

ダイナミック割り当てから複数の IP アドレス範囲を除外することができます。

例

ダイナミック割り当てから IP アドレス 10.110.1.1～10.110.1.63 を除外します。

<AP> system-view

[AP] dhcp server forbidden-ip 10.110.1.1 10.110.1.63

関連コマンド

- **forbidden-ip**
- **static-bind**

9.2.9 dhcp server ip-pool

Syntax

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

pool-name: アドレスプールを固有に識別するため DHCP アドレスプールの名前を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

dhcp server ip-pool コマンドは DHCP アドレスプールを作成し、その view に移行します。

undo dhcp server ip-pool コマンドは指定した DHCP アドレスプールを削除します。

またコマンドを使用して既存の DHCP アドレスプールに移行することができます。

DHCP アドレスプールは DHCP クライアントに割り当てられる設定パラメータを記録するために使用されます。

例

DHCP アドレスプール pool1 を作成します。

<AP> system-view

[AP] dhcp server ip-pool pool1

[AP-dhcp-pool-pool1]

関連コマンド

- **dhcp server apply ip-pool**
- **display dhcp server pool**

9.2.10 dhcp server ping packets

Syntax

dhcp server ping packets *number*

undo dhcp server ping packets

デフォルト

1

View

System view

定義済みユーザロール

network-admin

パラメータ

number: ping パケットの最大数を指定します。設定範囲は 0～10 です。0 は DHCP サーバがアドレス競合の検出を行わないことを示します。

説明

dhcp server ping packets コマンドは ping パケットの最大数を指定します。

undo dhcp server ping packets コマンドはデフォルトに戻します。

IP アドレスの競合を防ぐため、DHCP サーバは DHCP クライアントに IP アドレスを割り当てる前に IP アドレス宛に ping を実行します。

ping が成功した場合、サーバは IP アドレスが競合していると認識し、新しい IP アドレスを選択します。すべての ping が失敗すると、サーバは DHCP クライアントに IP アドレスを割り当てます。

例

ping パケットの最大数を 10 に指定します。

<AP> system-view

[AP] dhcp server ping packets 10

関連コマンド

- **dhcp server ping timeout**
- **display dhcp server conflict**
- **reset dhcp server conflict**

9.2.11 dhcp server ping timeout

Syntax

dhcp server ping timeout *milliseconds*

undo dhcp server ping timeout

デフォルト

500 ミリ秒

View

System view

定義済みユーザロール

network-admin

パラメータ

milliseconds: ping 応答に対するタイムアウト時間を指定します。設定範囲は 0～10000 ミリ秒です。アドレス競合の検出を無効にする場合、0 を指定します。

説明

dhcp server ping timeout コマンドは DHCP サーバで ping 応答に対するタイムアウト時間を設定します。

undo dhcp server ping timeout コマンドはデフォルトに戻します。

IP アドレスの競合を防ぐため、DHCP サーバは DHCP クライアントに IP アドレスを割り当てる前に IP アドレス宛に ping を実行します。

ping が成功した場合、サーバは IP アドレスが競合していると認識し、新しい IP アドレスを選択します。すべての ping が失敗すると、サーバは DHCP クライアントに IP アドレスを割り当てます。

例

ping 応答に対するタイムアウト時間を 1000 ミリ秒に設定します。

<AP> system-view

[AP] dhcp server ping timeout 1000

関連コマンド

- **dhcp server ping packets**
- **display dhcp server conflict**
- **reset dhcp server conflict**

9.2.12 dhcp server relay information enable

Syntax

dhcp server relay information enable

undo dhcp server relay information enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

dhcp server relay information enable コマンドは DHCP サーバのオプション 82 を有効にします。

undo dhcp server relay information enable コマンドは DHCP サーバのオプション 82 を無効にします。

DHCP サーバがオプション 82 を処理するように設定されている場合、オプション 82 のメッセージを受信すると、DHCP サーバはオプション 82 を DHCP 応答メッセージに追加します。DHCP サーバがオプション 82 を無効するように設定されている場合、DHCP 応答メッセージにオプション 82 を追加しません。

例

DHCP サーバのオプション 82 を無効にします。

<AP> system-view

[AP] undo dhcp server relay information enable

9.2.13 display dhcp server conflict

Syntax

display dhcp server conflict [**ip** *ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定した IP アドレスの競合情報を表示します。指定しない場合、すべての IP アドレスの競合情報を表示します。

説明

display dhcp server conflict コマンドは IP アドレス競合の情報を表示します。

DHCP サーバは以下の状況で IP アドレス競合の情報を作成します。

- DHCP クライアントに IP アドレスを割り当てる前、DHCP サーバは ping を行い、が他のホストで IP アドレスを使用しているかどうかを検出します。
- DHCP クライアントは IP アドレス競合をサーバに通知するため、DHCP サーバに DECLINE パケットを送信します。
- DHCP サーバはアドレスプールの割り当て可能なアドレスが自身の IP アドレスであることを検出します。

例

すべての IP アドレスの競合情報を表示します。

<AP> display dhcp server conflict

```
IP address         Detect time
4.4.4.1            Apr 25 16:57:20 2007
4.4.4.2            Apr 25 17:00:10 2007
```

表 9-1 コマンド出力

フィールド	説明
IP address	競合したIPアドレスです。
Detect time	競合が検出された時間です。

関連コマンド

reset dhcp server conflict

9.2.14 display dhcp server expired

Syntax

display dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定した IP アドレスのリース期限の終了に関する情報を表示します。指定しない場合、すべての IP アドレスのリース期限の終了に関する情報を表示します。

pool *pool-name*: 指定したアドレスプールのリース期限の終了に関する情報を表示します。設定範囲は 1～63 です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールのリース期限の終了に関する情報を表示します。

説明

display dhcp server expired コマンドはリース期限の終了に関する情報を表示します。

有効なアドレスがすべて割り当てられてとき、DHCP サーバは DHCP クライアントにリース期限が終了した IP アドレスを割り当てます。

例

すべてのリース期限の終了に関する情報を表示します。

<AP> display dhcp server expired

```
IP address      Client-identifier/Hardware address   Lease expiration
4.4.4.6         3030-3066-2e65-3230-302e-3130-3234   Apr 25 17:10:47 2007
               -2d45-7468-6572-6e65-7430-2f31
```

表 9-2 コマンド出力

フィールド	説明
IP address	リース期限が終了するIPアドレスです。
Client-identifier/Hardware address	クライアントIDあるいはMACアドレスです。 DHCP client ID • クライアントIDの値がASCII形式である場合、タイプは00です。 • クライアントIDの値が指定したインタフェースのMACアドレスを使用している場合、タイプは01です。 • クライアントIDの値が16進数形式である場合、タイプは文字列の最初の2桁の文字です。
Lease expiration	リース期限が終了する時間です。

関連コマンド

reset dhcp server expired

9.2.15 display dhcp server free-ip

Syntax

display dhcp server free-ip [**pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool *pool-name*: 指定したアドレスプールの割り当て可能な IP アドレスを表示します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの割り当て可能なすべての IP アドレスを表示します。

説明

display dhcp server free-ip コマンドは割り当て可能な IP アドレスを表示します。

例

すべてのアドレスプールの割り当て可能な IP アドレスを表示します。

<AP> display dhcp server free-ip

```
Pool name: 1
  Network: 10.0.0.0 mask 255.0.0.0
    IP ranges from 10.0.0.10 to 10.0.0.100
    IP ranges from 10.0.0.105 to 10.0.0.255
  Secondary networks:
    10.1.0.0 mask 255.255.0.0
      IP ranges from 10.1.0.0 to 10.1.0.255
    10.2.0.0 mask 255.255.0.0
      IP Ranges from 10.2.0.0 to 10.2.0.255

Pool name: 2
  Network: 20.1.1.0 mask 255.255.255.0
    IP ranges from 20.1.1.0 to 20.1.1.255
```

表 9-3 コマンド出力

フィールド	説明
Pool name	アドレスプールの名前です。

フィールド	説明
Network	割り当て可能なネットワークです。
IP ranges	割り当て可能なIPアドレス範囲です。
Secondary networks	割り当て可能なセカンダリネットワークです。

関連コマンド

- **address range**
- **dhcp server ip-pool**
- **network**

9.2.16 display dhcp server ip-in-use

Syntax

display dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip *ip-address*: 指定した IP アドレスの割り当て情報を表示します。指定しない場合、すべての割り当てられた IP アドレスの情報を表示します。

pool *pool-name*: 指定した IP アドレスプールの割り当て情報を表示します。設定範囲は 1～63 です。大文字、小文字を区別しません。指定しない場合、すべての割り当てられた IP アドレスプールの IP アドレスの情報を表示します。

説明

display dhcp server ip-in-use コマンドは割り当てられた IP アドレスの情報を表示します。

クライアントの割り当て情報は、DHCP サーバに DHCP クライアントのゲートウェイが設定されているときのみ、IP ソースガードのような他のセキュリティモジュールで使用することができます。

リース期限が 2100 年を超過する場合、リース期限は After 2100 と表示されます。

例

すべての割り当てられた DHCP アドレスの情報を表示します。

<AP> display dhcp server ip-in-use

```
IP address      Client identifier/    Lease expiration      Type
                Hardware address
10.1.1.1        4444-4444-4444        Not used              Static(F)
10.1.1.2        3030-3030-2e30-3030-  May 1 14:02:49 2015   Auto(C)
                662e-3030-3033-2d45-
                7468-6572-6e65-74
10.1.1.3        1111-1111-1111        After 2100            Static(C)
```

表 9-4 コマンド出力

フィールド	説明
IP address	割り当てられたIPアドレスです。
Client identifier/Hardware address	クライアントIDあるいはハードウェアアドレスです。クライアントIDは16進数の文字列で指定され、最初の2文字はハードウェアタイプの値を表します。 • ASCII文字列を使用する場合、ハードウェアタイプの値は00で、タイプがないことを意味します。 • ハードウェアタイプがEthernetの場合、タイプの値は01です。 • ハードウェアタイプがトークンリングの場合、タイプの値は06です。
Lease expiration	リース期間です。 • **Exact time (May 1 14:02:49 2015)**—リース期間が終了する時間です。 • **Not used**—スタティック割り当てのIPアドレスがクライアントに割り当てられていません。 • **Unlimited**—期限なしのリースです。 • **After 2100**—リース期間の終了が2100年以降です。
Type	割り当てタイプです。 • **Static(F)**— IPアドレスが割り当てられていない空きのスタティック割り当てです。 • **Static(O)**—IPアドレスが選択され、提供されたスタティック割り当てです。DHCPサーバによってDHCP-OFFERパケットにIPアドレスが記載されDHCPクライアントに送信されます。 • **Static(C)**—IPアドレスがDHCPクライアントに割り当てられ、コミットされたスタティック割り当てです。

フィールド	説明
	• **Auto(O)**—IPアドレスが選択され、一時的に提供されたダイナミック割り当てです。DHCPサーバによってDHCP-OFFERパケットにIPアドレスが記載されDHCPクライアントに送信されます。 • **Auto(C)**— IPアドレスがDHCPクライアントに割り当てられ、コミットされたダイナミック割り当てです。

関連コマンド

reset dhcp server ip-in-use

9.2.17 display dhcp server pool

Syntax

display dhcp server pool [*pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool-name: 指定したアドレスプールの情報を表示します。設定範囲は 1〜63 文字です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの情報を表示します。

説明

display dhcp server pool コマンドは DHCP アドレスプールの情報を表示します。

例

すべての DHCP アドレスプールの情報を表示します。

<AP> display dhcp server pool

```
Pool name: 0
  Network 20.1.1.0 mask 255.255.255.0
  class a range 20.1.1.50 20.1.1.60
  bootfile-name abc.cfg
  dns-list 20.1.1.66 20.1.1.67 20.1.1.68
  domain-name www.aabbcc.com
  bims-server ip 192.168.0.51 sharekey cipher $c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  option 2 ip-address 1.1.1.1
  expired 1 2 3 0

Pool name: 1
  Network 20.1.1.0 mask 255.255.255.0
  secondary networks:
    20.1.2.0 mask 255.255.255.0
    20.1.3.0 mask 255.255.255.0
  bims-server     ip     192.168.0.51     port     50     sharekey     cipher
$c$3$K13OmQPi791YvQoF2Gs1E+65LOU=
  forbidden-ip 20.1.1.22 20.1.1.36 20.1.1.37
  forbidden-ip 20.1.1.22 20.1.1.23 20.1.1.24
```

```
  gateway-list 1.1.1.1 2.2.2.2 4.4.4.4
  nbns-list 5.5.5.5 6.6.6.6 7.7.7.7
  netbios-type m-node
  option 2 ip-address 1.1.1.1
  expired 1 0 0 0

Pool name: 2
  Network 20.1.1.0 mask 255.255.255.0
  address range 20.1.1.1 to 20.1.1.15
  class departmentA range 20.1.1.20 to 20.1.1.29
  class departmentB range 20.1.1.30 to 20.1.1.40
  next-server 20.1.1.33
  tftp-server domain-name www.dian.org.cn
  tftp-server ip-address 192.168.0.120
  voice-config ncp-ip 10.1.1.2
  voice-config as-ip 10.1.1.5
  voice-config fail-over 10.1.1.1 123*
  option 2 ip-address 1.1.1.3
  expired 1 0 0 0

Pool name: 3
  static bindings:
    ip-address 10.10.1.2 mask 255.0.0.0
      hardware-address 00e0-00fc-0001 ethernet
    ip-address 10.10.1.3 mask 255.0.0.0
      client-identifier aaaa-bbbb
  expired unlimited
```

表 9-5 コマンド出力

フィールド	説明
Pool name	アドレスプールの名前です。 • **lock**—ルーズモードでロックされています。サーバは、プール内のIPアドレスに対するオンラインDHCPクライアントからのリース更新要求に応答しますが、プール内のIPアドレスを新しいDHCPクライアントに割り当てません。 • **lock strict**—strictモードでロックされます。サーバは、プール内のIPアドレスに対するオンラインDHCPクライアントからのリース更新要求に応答したり、プール内のIPアドレスを新しいDHCPクライアントに割り当てたりしません。IPプールをロックしない場合、このコマンドはロック状態情報を表示しません。 IPプールをロックしない場合、このコマンドはロック状態情報を表示しません。
Network	割り当て可能なネットワークです。
secondary networks	割り当て可能なセカンダリネットワークです。
address range	割り当て可能なアドレス範囲です。
class *class-name* range	DHCPユーザクラスとアドレス範囲です。
static bindings	スタティックIP-MAC/クライアントIDバインディングです。
ip-address mask	スタティックバインディングのIPアドレスとマスクです。
hardware-address	スタティックバインディングのハードウェアアドレスです。
client-identifier	スタティックバインディングのクライアントIDです。
description	スタティックバインディングの説明です。
option	カスタマイズされたDHCPオプションです。
expired	リース期限です。この例の1 2 3 4は1日2時間3分4秒を示します。
bootfile-name	ブートファイル名です。
dns-list	DNSサーバのIPアドレスです。
domain-name	ドメイン名サフィックスです。

フィールド	説明
bims-server	BIMSサーバの情報です。
forbidden-ip	ダイナミックの割り当てから除外されたIPアドレスです。
forbidden-ip-range	ダイナミックの割り当てから除外されるIPアドレス範囲です。
gateway-list	ゲートウェイアドレスです。
nbns-list	WINSサーバのアドレスです。
netbios-type	NetBIOSノードタイプです。
next-server	次のサーバのIPアドレスです。
tftp-server domain-name	TFTPサーバ名です。
tftp-server ip-address	TFTPサーバのアドレスです。
voice-config ncp-ip	プライマリのネットワークコーリングプロセッサのアドレスです。
voice-config as-ip	バックアップのネットワークコーリングプロセッサのアドレスです。
voice-config voice-vlan	音声VLANです。
voice-config fail-over	フェイルオーバルートです。

9.2.18 display dhcp server statistics

Syntax

display dhcp server statistics [**pool** *pool-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pool *pool-name*: アドレスプールを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの情報を表示します。

説明

display dhcp server statistics コマンドは DHCP サーバの統計情報を表示します。

例

DHCP サーバの統計情報を表示します。

<AP> display dhcp server statistics

```
Pool number:                    1
Pool utilization:               0.39%
Bindings:
  Automatic:                    1
  Manual:                       0
  Expired:                      0
Conflict:                       1
Messages received:              10
  DHCPDISCOVER:                 5
  DHCPREQUEST:                  3
  DHCPDECLINE:                  0
  DHCPRELEASE:                  2
  DHCPINFORM:                   0
  BOOTPREQUEST:                 0
Messages sent:                  6
  DHCPOFFER:                    3
  DHCPACK:                      3
  DHCPNAK:                      0
  BOOTPREPLY:                   0
Bad Messages:                   0
```

表 9-6 コマンド出力

フィールド	説明
Pool number	アドレスプールの総数です。このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Pool utilization	プール使用率です。 ● すべてのアドレスプールの統計情報を表示する場合、すべてのアドレスプールの使用率を表示します。 ● アドレスプールの統計情報を表示する場合、指定したアドレスプールの使用率を表示します。
Bindings	以下のタイプの割り当てです。 ● **Automatic**—ダイナミック割り当て数です。 ● **Manual**—スタティック割り当て数です。 ● **Expired**—除外された割り当て数です。
Conflict	競合アドレスの総数です。このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Messages received	クライアントから受信されたDHCPパケットです。 ● DHCPDISCOVER ● DHCPREQUEST ● DHCPDECLINE ● DHCPRELEASE ● DHCPINFORM ● BOOTPREQUEST このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Messages sent	クライアントに送信されたDHCPパケットです。 ● DHCPOFFER ● DHCPACK ● DHCPNAK ● BOOTPREPLY このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。
Bad Messages	BADメッセージ数です。 このフィールドは指定したアドレスプールの統計情報を表示する場合、表示されません。

関連コマンド

reset dhcp server statistics

9.2.19 dns-list

Syntax

dns-list *ip-address*&<1-8>

undo dns-list [*ip-address*&<1-8>]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: DNS サーバを指定します。&<1-8>は DNS サーバのアドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを指定します。

undo dns-list コマンドは DHCP アドレスプールの DNS サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

パラメータを指定しない場合、**undo dns-list** コマンドは DHCP アドレスプールのすべての DNS サーバのアドレスを削除します。

例

DHCP アドレスプール 0 の DNS サーバアドレス 10.1.1.254 を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] dns-list 10.1.1.254

関連コマンド

display dhcp server pool

9.2.20 domain-name

Syntax

domain-name *domain-name*

undo domain-name

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名を指定します。設定範囲は 1～50 です。大文字、小文字を区別します。

説明

domain-name コマンドは DHCP アドレスプールのドメイン名を指定します。

undo domain-name コマンドは DHCP アドレスプールのドメイン名を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 のドメイン名 company.com を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] domain-name company.com

関連コマンド

display dhcp server pool

9.2.21 expired

Syntax

expired { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }

undo expired

デフォルト

1 日

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

day *day*: 日数を指定します。設定範囲は 0～365 日です。

hour *hour*: 時間を指定します。設定範囲は 0～23 時間です。デフォルトは 0 時間です。

minute *minute*: 分を指定します。設定範囲は 0～59 分です。デフォルトは 0 分です。

second *second*: 秒を指定します。設定範囲は 0～59 秒です。デフォルトは 0 秒です。

unlimited: リース期間を指定しません。正確には 136 年のリース期間です。

説明

expired コマンドは DHCP アドレスプールのリース期間を指定します。

undo expired コマンドは DHCP アドレスプールのリース期間をデフォルトに戻します。

DHCP サーバは DHCP クライアントにリース期間と共に IP アドレスを割り当てます。リース期間が終了する前に、DHCP クライアントはリース期間を延長する必要があります。

- リース期間の延長が成功した場合、DHCP クライアントは IP アドレスを使用し続けることができます。
- リース期間の延長が失敗したとき、以下のイベントの両方が発生します。
  - リース期間が終了した後 DHCP クライアントは IP アドレスを使用することができません。
  - DHCP サーバは終了したアドレスとして IP アドレスにラベルをつけます。

例

DHCP アドレスプール 0 のリース期間を 1 日、2 時間、3 分、4 秒に指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] expired day 1 hour 2 minute 3 second 4

関連コマンド

- **display dhcp server expired**
- **display dhcp server pool**
- **reset dhcp server expired**

9.2.22 forbidden-ip

Syntax

forbidden-ip *ip-address*&<1-8>

undo forbidden-ip [*ip-address*&<1-8>]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: 除外する IP アドレスを指定します。&<1-8>は IP アドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

forbidden-ip コマンドはアドレスプールのダイナミック割り当てから IP アドレスを除外します。

undo forbidden-ip コマンドは設定を削除します。

アドレスプールの除外された IP アドレスは他のアドレスプールで割り当て可能です。

アドレスプールで最大 4096 の IP アドレスを除外することができます。

パラメータを指定しない場合、**undo forbidden-ip** コマンドはすべての除外した IP アドレスを削除します。

例

DHCP アドレスプール 0 のダイナミック割り当てから 192.168.1.3 と 192.168.1.10 を除外します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] forbidden-ip 192.168.1.3 192.168.1.10

関連コマンド

- **dhcp server forbidden-ip**
- **display dhcp server pool**

9.2.23 gateway-list

Syntax

gateway-list *ip-address*&<1-64> [export-route]

undo gateway-list [*ip-address*&<1-64>] [export-route]

デフォルト

設定なし

DHCP address pool または DHCP secondary subnet にはゲートウェイ アドレスが構成されていません。

View

DHCP address pool view

DHCP secondary subnet view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-64>: ゲートウェイを指定します。&<1-64>はゲートウェイアドレスを半角スペースで区切り最大 64 つまで指定できることを示します。ゲートウェイアドレスは割り当て可能な IP アドレスと同一のサブネットに存在する必要があります。

export-route: アドレス管理モジュール内のデバイスの MAC アドレスにゲートウェイをバインドします。ARP モジュールは、エントリを使用して DHCP クライアントからの ARP 要求に応答します。このキーワードを指定しない場合、ゲートウェイはデバイスの MAC アドレスにバインドされません。

説明

Gateway-list を使用して、DHCP address pool または DHCP secondary subnet 内のゲートウェイ アドレスを指定します。

undo gateway-list を使用して、指定されたゲートウェイ アドレスを DHCP address pool または DHCP secondary subnet から削除します。

DHCP サーバは、次の方法で secondary subnet 上のクライアントにゲートウェイ アドレスを割り当てます。

· ゲートウェイが address pool view と secondary subnet view の両方で指定されている場合、DHCP は secondary subnet view で指定されたゲートウェイを割り当てます。

· ゲートウェイが address pool view で指定されているが、secondary subnet view では指定されていない場合、DHCP は address pool view で指定されたゲートウェイを割り当てます。

パラメータを何も指定しない場合、**undo gateway-list** コマンドはすべてのゲートウェイ アドレスを削除します。

例

DHCP address pool 0 にゲートウェイ アドレス 10.1.1.1 を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] gateway-list 10.1.1.1

関連コマンド

display dhcp server pool

9.2.24 if-match

Syntax

if-match rule *rule-number* **{ hardware-address** *hardware-address* **mask** *hardware-address-mask* **| option** *option-code* **[ascii** *ascii-string* **[offset** *offset* **| partial] | hex** *hex-string* **[mask** *mask* **| offset** *offset* **length** *length* **| partial]] | relay-agent** *gateway-address* **}**

undo if-match rule *rule-number*

デフォルト

設定なし

View

DHCP user class view

定義済みユーザロール

network-admin

パラメータ

rule *rule-number*: ルールに割り当てる ID を指定します。値の範囲は 1～128 までで、ID が小さいほど、一致の優先度が高くなります。

hardware-address *hardware-address*: ハードウェアアドレスをハイフンで区切られた 16 進数の文字列で指定します。値の範囲は 4～39 文字です。最後の 16 進数は 2 桁または 4 桁で、その他の 16 進数は 4 桁である必要があります。たとえば、aabb-ccdd-ee は有効で、aabb-c-dddd または aabb-cc-dddd は無効です。

mask *hardware-address-mask*: *hardware-address* と AND 演算するマスクを指定します。マスクの長さはハードウェアアドレスと同じである必要があります。

option *option-code*: DHCPオプションの番号を指定します。1～254 の数値で指定します。

ascii *ascii-string*: ASCII 文字列を指定します。1～128 文字の文字列で指定します。

offset *offset*: 一致操作が開始されるまでのオフセットをバイト単位で指定します。値の範囲は 0～254 です。オフセット値を指定しない場合は、オプション内容の先頭バイトから照合が開始されます。ASCII 文字列を指定した場合、オフセット後のオプションの内容が ASCII 文字列と同じであれば、パケットはルールに一致します。16 進数を指定した場合、オフセット後の指定した長さのオプション内容が 16 進数と同じであれば、パケットはルールに一致します。

partial: 部分一致を有効にします。パケット内の指定されたオプションに、ルールで指定された ASCII 文字列または 16 進数が含まれている場合、パケットはルールに一致します。たとえば、ルールで abc を指定した場合、オプションの内容 xabc、xyzabca、xabcyz、および abcxyz はすべてルールに一致します。

hex *hex-string*: 16 進数の文字列を指定します。16 進数の文字列の長さは 2～256 までの偶数である必要があります。

mask *mask*: 一致操作の 16 進数マスクを指定します。マスク長は 2～256 までの偶数で、*hex-string* の文字列長と同じである必要があります。DHCP サーバは、マスク長のオプション内容を先頭から選択し、選択したオプション内容と指定した 16 進数をマスクと AND 演算します。2 つの AND 演算結果が同じ場合、パケットはルールと一致します。

length *length*: 照合するオプション内容の長さをバイト単位で指定します。値の範囲は 1～128 です。長さは、16 進文字列の長さと同じである必要があります。

relay-agent *gateway-address*: giaddr フィールドの値を指定します。値はドット付き 10 進表記の IPv 4 アドレスです。パケットの giaddr フィールド値がルールの値と同じ場合、パケットはルールに一致します。

説明

if-match コマンドは DHCP ユーザクラスの一致ルールを設定します。

undo if-match コマンドは DHCP ユーザクラスの一致ルールを削除します。

DHCP クライアントから送信された DHCP-DISCOVER パケットが DHCP ユーザクラスのルールと一致する場合、DHCP クライアントはユーザクラスと一致します。

1 つの DHCP ユーザクラスに対して複数の一致ルールを設定できます。

各一致ルールは、そのタイプ内のルール ID によって一意に識別されます(ハードウェアアドレス、オプション、またはリレーエージェントアドレス)。

- 設定しているルールの ID とタイプが既存のルールと同じ場合、新しいルールによって既存のルールが上書きされます。
- 設定するルールの ID が既存のルールと同じで、タイプが異なる場合は、新しいルールが有効になり、既存のルールと共存します。ベストプラクティスとして、異なるタイプのルールに同じ ID を割り当てないでください。
- 異なる ID のルールが同じルール内容を持つことはできません。

if-match hardware-address ルールを設定する場合は、次の注意事項に従ってください。

- ハードウェアアドレスタイプは、MAC アドレスのみをサポートします。他のタイプのハードウェアアドレスを持つクライアントでは、ルール一致となりません。
- 指定されたハードウェアアドレスは、クライアントハードウェアアドレスと同じ長さである必要があります。MAC アドレスと一致させるには、指定するハードウェアアドレスの長さを 6 バイトにする必要があります。
- ハードウェアアドレスのマスク内の、f と 0 は不連続にすることができます。たとえば、if-match rule 1 hardware-address 0094-0000-1100 mask ffff-0000-ff00 は、最初の 2 バイトが 0094 で、5 バイトが 11 のハードウェアアドレスと一致します。

if-match オプションルールを設定する場合は、次の注意事項に従ってください。

- オプションを含むパケットを照合するには、*option-code* の引数だけを指定します。
- AND 演算で 16 進数を一致させるには、option-code hex-string mask オプションを指定します。

- 16 進数を直接照合するには、オプション *option-code hex-string* [**offset** *offset* **length** *length* [**partial**] オプションを指定します。offset、length、または partial パラメータを指定しない場合、オプションの内容が 16 進数で始まると、パケットはルールに一致します。
- ASCII 文字列と一致させるには、*option-code* **ascii** *ascii-string* [**offset** *offset* [partial] オプションを指定します。offset または partial パラメータを指定しない場合、オプションの内容が ASCII 文字列で始まると、パケットはルールに一致します。

例

DHCP ユーザクラス test を作成し、その View に移行します。

<AP> system-view

[AP] dhcp class test

[AP-dhcp-class-test]

関連コマンド

- **class option-group**
- **if-match**

9.2.25 nbns-list

Syntax

nbns-list *ip-address*&<1-8>

undo nbns-list [*ip-address*&<1-8>]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address&<1-8>: WINS サーバの IP アドレスを指定します。&<1-8>は WINS サーバアドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

nbns-list コマンドは DHCP アドレスプールの WINS サーバアドレスを指定します。

undo nbns-list コマンドは指定した WINS サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

パラメータを指定しない場合、**undo nbns-list** コマンドはすべての WINS サーバアドレスを削除します。

例

DHCP アドレスプール 0 の WINS サーバアドレス 10.1.1.1 を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] nbns-list 10.1.1.1

関連コマンド

- **display dhcp server pool**
- **netbios-type**

9.2.26 netbios-type

Syntax

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

b-node: ブロードキャストノードを指定します。b-node クライアントはサーバから名前-IP マッピングを取得するため、ブロードキャストメッセージで宛先名を送信します。

h-node: ハイブリッドノードを指定します。h-node クライアントは WINS サーバに宛先名をユニキャストします。応答を受信しない場合、h-node クライアントはサーバからマッピングを取得するため宛先名をブロードキャストします。

m-node: ミックスノードを指定します。m-node クライアントは宛先名をブロードキャストします。応答を受信しない場合、m-node クライアントはサーバからマッピングを取得するため宛先名をユニキャストします。

p-node: ピアツーピアノードを指定します。p-node クライアントは WINS サーバから WINS サーバを取得するため、ユニキャストメッセージの宛先アドレスを送信します。

説明

netbios-type コマンドはDHCPアドレスプールのNetBIOSノードタイプを指定します。

undo netbios-type コマンドは指定した NetBIOS ノードタイプを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 の NetBIOS ノードタイプを p-node に指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] netbios-type p-node

関連コマンド

- **display dhcp server pool**
- **nbns-list**

9.2.27 network

Syntax

network *network-address* [*mask-length* | **mask** *mask*] [**secondary**] [**export-route**]

undo network *network-address* [*mask-length* | **mask** *mask*] [**secondary**]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

network-address: ダイナミック割り当てのサブネットを指定します。マスク長やマスクが指定されない場合、ナチュラルマスクが使用されます。

mask-length: マスク長を指定します。設定範囲は 1〜30 です。

mask *mask*: ドットで区切られた形式でマスクを指定します。

secondary: セカンダリサブネットを指定します。指定しない場合、プライマリサブネットを指定します。プライマリサブネットのアドレスが使い果たされている場合、DHCP サーバはクライアントのためにセカンダリサブネットからアドレスを選択します。

export-route: DHCP クライアントに割り当てられたサブネットをアドバタイズします。このキーワードを指定しない場合、サブネットはアドバタイズされません。

説明

network コマンドは DHCP アドレスプールのダイナミック割り当てのサブネットを指定します。

undo network コマンドは指定されたサブネットを削除します。

セカンダリサブネットを指定し、その view に移行するため、**secondary** を使用することができます。**gateway-list** コマンドを使用して DHCP クライアントのためにセカンダリサブネットのゲートウェイを指定することができます。

DHCP アドレスプールで 1 つのプライマリサブネットのみを指定することができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

DHCP アドレスプールで最大 32 のセカンダリサブネットを指定することができます。

DHCP アドレスプールのプライマリサブネットとセカンダリサブネットは同一ネットワークアドレス、マスクにすることができません。

アドレスプールで **address range** コマンドを使用した場合、同一のアドレスプールのセカンダリサブネットを指定することができません。

ネットワークの設定の変更あるいは削除を行うと現在のアドレスプールから割り当てられたアドレスを削除します。

export-route コマンドを複数回実行すると、最新の設定が有効になります。

例

DHCP アドレスプール 0 のプライマリサブネット 192.168.8.0/24 とセカンダリサブネット 192.168.10.0/24 を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0

[AP-dhcp-pool-0] network 192.168.10.0 mask 255.255.255.0 secondary

[AP-dhcp-pool-0-secondary]

関連コマンド

- **display dhcp server pool**
- **gateway-list**

9.2.28 next-server

Syntax

next-server *ip-address*

undo next-server

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address: サーバの IP アドレスを指定します。

説明

next-server コマンドは DHCP アドレスプールのサーバの IP アドレスを指定します。

undo next-server コマンドは DHCP アドレスプールからサーバの IP アドレスを削除します。

起動時、DHCP クライアントは IP アドレス、指定されたサーバの IP アドレスを取得します。他のブート情報を取得するため TFTP サーバのような指定されたサーバと連絡をとります。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 のサーバの IP アドレス 10.1.1.254 を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] next-server 10.1.1.254

関連コマンド

display dhcp server pool

9.2.29 option

Syntax

option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address*&<1-8> }

undo option *code*

デフォルト

設定なし

View

DHCP address pool view

DHCP option group view

定義済みユーザロール

network-admin

パラメータ

code: 自己定義されたオプション数を指定します。設定範囲は 2～254 です。50～54、56、58、59、61、62、82 を除きます。

ascii *ascii-string*: ASCII の文字列を指定します。設定範囲は 1～255 です。

hex *hex-string*: 16 進数の偶数番号を指定します。設定範囲は 2～256 です。

ip-address *ip-address*&<1-8>: 自己定義されたオプションの IP アドレスを指定します。&<1-8>は IP アドレスを半角スペースで区切り最大 8 つまで指定できることを示します。

説明

option コマンドは自己定義された DHCP オプションを設定します。

undo option コマンドは自己定義された DHCP オプションを削除します。

DHCP サーバは ASCII 文字列、16 進数文字列、IP アドレスで自己定義されたオプションを記載し、DHCP 応答の自己定義されたオプションをクライアントに送信します。

以下の目的のためにオプションを定義することができます。

- 新しくリリースされたオプションを追加します。
- オプション 43 のようなベンダ指定のオプションを追加します。
- CLI によって設定できない、専用の設定コマンドのオプションを追加します。たとえば **option** *4* **ip-address** *1.1.1.1* コマンドで DHCP クライアントにタイムサーバアドレス 1.1.1.1 を定義することができます。
- DHCP オプションでは正確な要件を満たすことができない場合、既存の DHCP オプションを拡張します。たとえば、**dns-list** コマンドは 8 つの DNS サーバアドレスを設定することができます。8 つを超える DNS サーバを指定する場合、すべての DNS サーバで **option** *6* コマンドを使用する必要があります。

専用のコマンドと **option** コマンドの両方を使用して DHCP オプションを指定する場合、DHCP サーバは専用のコマンドで指定された内容を割り当てます。たとえば、DHCP サーバのアドレスが **dns-list** コマンドと **option** *6* コマンドで指定された場合、サーバは **dns-list** コマンドで指定されたアドレスを使用します。

DHCP オプショングループで設定された DHCP オプションは DHCP アドレスプールで設定された DHCP オプションより優先されます。

option コマンドで同じコードが指定された場合、最後に行った設定が適用されます。

例

アドレスプール 0 のログサーバアドレス 2.2.2.2 を指定するためオプション 7 を設定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] option 7 ip-address 2.2.2.2

関連コマンド

display dhcp server pool

9.2.30 reset dhcp server conflict

Syntax

reset dhcp server conflict [**ip** *ip-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 指定された IP アドレスの競合に関する情報を削除します。指定しない場合、すべてのアドレスの競合に関する情報を削除します。

説明

reset dhcp server conflict コマンドは IP アドレスの競合に関する情報を削除します。

ダイナミックに割り当てられた IP アドレスが他のホストでスタティックに設定されたとき、アドレスの競合が発生します。アドレスプールの設定を修正した後、競合したアドレスは割り当て可能になります。これらのアドレスを割り当てるため、最初に競合に関する情報を削除するため、**reset dhcp server conflict** コマンドを使用します。

例

すべてのアドレスの競合に関する情報を削除します。

<AP> reset dhcp server conflict

関連コマンド

display dhcp server conflict

9.2.31 reset dhcp server expired

Syntax

reset dhcp server expired [**ip** *ip-address* | **pool** *pool-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 期限が終了した IP アドレスを指定し、IP アドレスに関する割り当て情報を削除します。指定しない場合、すべてのアドレスの競合に関する情報を削除します。

pool *pool-name*: 指定したアドレスプールの期限が終了した IP アドレスの割り当て情報を削除します。設定範囲は 1～63 です。大文字、小文字は区別しません。指定しない場合､すべてのアドレスプールの期限が終了した IP アドレスの割り当て情報を削除します。

説明

reset dhcp server expired コマンドは期限が終了した IP アドレスの割り当て情報を削除します。

例

すべての期限が終了した IP アドレスの割り当て情報を削除します。

<AP> reset dhcp server expired

関連コマンド

display dhcp server expired

9.2.32 reset dhcp server ip-in-use

Syntax

reset dhcp server ip-in-use [**ip** *ip-address* | **pool** *pool-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 指定した IP アドレスの割り当て情報を削除します。指定しない場合、すべての IP アドレスの割り当て情報を削除します。

pool *pool-name*: 指定したアドレスプールの割り当て情報を削除します。設定範囲は 1～63 です。大文字、小文字を区別しません。指定しない場合、すべてのアドレスプールの割り当て情報を削除します。

説明

reset dhcp server ip-in-use コマンドは IP アドレス、アドレスプールの割り当て情報を削除します。

reset dhcp server ip-in-use コマンドで割り当てられたスタティック割り当て情報を削除すると、スタティック割り当て情報は未割り当てのスタティック割り当て情報となります。

例

IP アドレス 10.110.1.1 の割り当て情報を削除します。

<AP> reset dhcp server ip-in-use ip 10.110.1.1

関連コマンド

display dhcp server ip-in-use

9.2.33 reset dhcp server statistics

Syntax

reset dhcp server statistics

View

User view

定義済みユーザロール

network-admin

説明

reset dhcp server statistics コマンドは DHCP サーバの統計情報を削除します。

例

DHCP サーバの統計情報を削除します。

<AP> reset dhcp server statistics

関連コマンド

display dhcp server statistics

9.2.34 static-bind

Syntax

static-bind ip-address *ip-address* [*mask-length* | **mask** *mask*] { **client-identifier** *client-identifier* | **hardware-address** *hardware-address* [**ethernet** | **token-ring**] } [**description** *description-text*]

undo static-bind ip-address *ip-address*

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address *ip-address*: スタティック割り当ての IP アドレスを指定します。マスク長あるいはマスクが指定されない場合、ナチュラルマスクが使用されます。

mask-length: マスク長を指定します。設定範囲は 1～30 です。

mask *mask*: ドットで区切られた形式でマスクを指定します。

client-identifier *client-identifier*: スタティック割り当てのクライアント ID を指定します。設定範囲は 4～254 文字です。形式は H-H-H で、16 進数の数字とハイフン（-）で構成されます。最後の H は 2 桁あるいは 4 桁の 16 進数にすることができますが、それ以外の H は 4 桁の 16 進数の文字にする必要があります。たとえば、aabb-cccc-dd は有効な ID ですが、aabb-c-dddd や aabb-cc-dddd は無効な ID です。

hardware-address *hardware-address*: スタティック割り当てのクライアントのハードウェアアドレスを指定します。設定範囲は 4～39 文字です。形式は H-H-H で、16 進数の数字とハイフン（-）で構成されます。最後の H は 2 桁あるいは 4 桁の 16 進数にすることができますが、それ以外の H は 4 桁の 16 進数の文字にする必要があります。たとえば、aabb-cccc-dd は有効なハードウェアアドレスですが、aabb-c-dddd や aabb-cc-dddd は無効なハードウェアアドレスです。

ethernet: クライアントのハードウェアアドレスのタイプを Ethernet に指定します。デフォルトタイプは Ethernet です。

token-ring: クライアントのハードウェアアドレスのタイプを Token Ring に指定します。

description *description-text*: スタティックバインディングの説明を指定します。1 文字以上 255 文字以下の文字列で、大文字と小文字が区別されます。

説明

static-bind コマンドはクライアント ID あるいは MAC アドレスを IP アドレスにスタティックに割り当てます。

undo static-bind コマンドはスタティックの割り当てを削除します。

スタティック割り当ての IP アドレスは DHCP サーバのインタフェースのアドレスにすることはできません。そうでなければ、IP アドレスの競合が発生すると、境界のクライアントは IP アドレスを取得することができません。

アドレスプールのスタティック割り当てを複数指定することができます。アドレスプールのスタティック割り当ては最大 8192 です。

スタティックの割り当てを修正することはできません。DHCP クライアントの割り当てを変更する場合、最初に既存の割り当てを削除し、新しい割り当てを作成してください。

例

DHCP アドレスプール 0 の IP アドレス 10.1.1.1/24 をクライアント ID が 00aa-aabb のクライアント ID に割り当てます。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0 client-identifier 00aa-aabb

関連コマンド

display dhcp server pool

9.2.35 tftp-server domain-name

Syntax

tftp-server domain-name *domain-name*

undo tftp-server domain-name

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

domain-name: TFTP サーバ名を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

説明

tftp-server domain-name コマンドは DHCP アドレスプールの TFTP サーバ名を指定します。

undo tftp-server domain-name コマンドは DHCP アドレスプールの TFTP サーバ名を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 の TFTP サーバ aaa を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] tftp-server domain-name aaa

関連コマンド

- **display dhcp server pool**
- **tftp-server ip-address**

9.2.36 tftp-server ip-address

Syntax

tftp-server ip-address *ip-address*

undo tftp-server ip-address

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

ip-address: TFTP サーバの IP アドレスを指定します。

説明

tftp-server ip-address コマンドは DHCP アドレスプールの TFTP サーバアドレスを指定します。

undo tftp-server ip-address コマンドは DHCP アドレスプールの TFTP サーバアドレスを削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 の TFTP サーバアドレス 10.1.1.1 を指定します。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] tftp-server ip-address 10.1.1.1

関連コマンド

- **display dhcp server pool**
- **tftp-server domain-name**

9.2.37 voice-config

Syntax

voice-config { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

デフォルト

設定なし

View

DHCP address pool view

定義済みユーザロール

network-admin

パラメータ

as-ip *ip-address*: バックアップのネットワークコーリングプロセッサの IP アドレスを指定します。

fail-over *ip-address dialer-string*: フェイルオーバ IP アドレスとダイヤル文字列を指定します。設定範囲は 1〜39 です。0〜9 の数字、アスタリスク（*）が含まれます。

ncp-ip *ip-address*: プライマリのネットワークコーリングプロセッサの IP アドレスを指定します。

voice-vlan *vlan-id*: 音声 VLAN ID を 2 から 4094 の範囲で指定します。

- **disable**: 指定した VLAN を無効にします。DHCP クライアントは、この VLAN を音声 VLAN として使用しません。
- **enable**: 指定した VLAN を有効にします。DHCP クライアントは、この VLAN を音声 VLAN として使用します。

説明

voice-config コマンドは DHCP アドレスプールのオプション 184 の内容を設定します。

undo voice-config コマンドは DHCP アドレスプールのオプション 184 の内容を削除します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

DHCP アドレスプール 0 のオプション 184 を設定します。プライマリのネットワークコーリングプロセッサの IP アドレスを 10.1.1.1、セカンダリのネットワークコーリングプロセッサの IP アドレスを 10.2.2.2 に設定します。フェイルオーバ IP アドレスは 10.3.3.3 です。ダイヤル文字列は 99*です。

<AP> system-view

[AP] dhcp server ip-pool 0

[AP-dhcp-pool-0] voice-config ncp-ip 10.1.1.1

[AP-dhcp-pool-0] voice-config as-ip 10.2.2.2

[AP-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*

関連コマンド

display dhcp server pool

9.3 DHCP リレーエージェント設定コマンド

9.3.1 dhcp relay client-information record

Syntax

dhcp relay client-information record

undo dhcp relay client-information record

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information record コマンドはリレーエントリのクライアント情報の記録を有効にします。

undo dhcp relay client-information コマンドはリレーエントリのクライアント情報の記録を無効にします。

DHCP リレーエージェントが DHCP クライアントのゲートウェイで設定されたときのみクライアント情報が記録されます。

リレーエントリはクライアントの IP アドレス、MAC アドレスのようなクライアントの情報が含まれます。

リレーエントリのクライアント情報の記録を無効にすると、記録されたすべてのリレーエントリを削除します。

例

リレーエントリのクライアント情報の記録を有効にします。

<AP> system-view

[AP] dhcp relay client-information record

関連コマンド

- **dhcp relay client-information refresh enable**

9.3.2 dhcp relay client-information refresh enable

Syntax

dhcp relay client-information refresh enable

undo dhcp relay client-information refresh enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

dhcp relay client-information refresh enable コマンドは DHCP リレーエージェントでダイナミックリレーエントリの定期的な更新を有効にします。

undo dhcp relay client-information refresh enable コマンドは DHCP リレーエージェントでダイナミックリレーエントリの定期的な更新を無効にします。

DHCP クライアントは DHCP サーバに IP アドレスをリリースするため、DHCP-RELEASE メッセージをユニキャストします。

DHCP リレーエージェントは DHCP サーバにメッセージを送信し、クライアントの IP-MAC アドレスエントリを削除しません。

この機能で、DHCP リレーエージェントは DHCP サーバに DHCP-REQUEST メッセージを定期的に送信するため、クライアントの IP アドレス、リレーインタフェースの MAC アドレスを使用します。

- サーバが DHCP-ACK メッセージを送信する、あるいは時間以内にメッセージを返信しない場合、DHCP リレーエージェントは以下の処理を行います。
  - □ リレーエントリを削除します。
  - □ IP アドレスをリリースするため、DHCP サーバに DHCP-RELEASE メッセージを送信します。
- サーバが DHCP-NAK メッセージを返信する場合、リレーエージェントはエントリを保持します。

この機能が無効である場合、DHCP リレーエージェントは自動でリレーエントリを削除しません。DHCP クライアントが IP アドレスをリリースしたのち、対応するリレーエントリを削除するため、リレーエージェントで **reset dhcp relay client-information** コマンドを使用する必要があります。

例

DHCP リレーエージェントでダイナミックリレーエントリの定期的な更新を無効にします。

<AP> system-view

[AP] undo dhcp relay client-information refresh enable

関連コマンド

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

9.3.3 dhcp relay information circuit-id

Syntax

dhcp relay information circuit-id { **bas** |**string** *circuit-id* | { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] [**interface**] } [**format** { **ascii** | **hex** }] }

undo dhcp relay information circuit-id

デフォルト

コードモードは normal で、パディング形式は hex です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

string *circuit-id*: circuit ID サブオプションの内容を指定します。設定範囲は 3～63 です。大文字、小文字を区別します。

normal: コードモードを normal モードに指定します。このパディングの内容は VLAN ID とポート番号から構成されます。

verbose: コードモードを verbose モードに指定します。このパディングの内容はノード識別子、インタフェース情報、VLAN ID が含まれます。デフォルトのノード識別子はアクセスノードの MAC アドレスです。デフォルトのインタフェース情報は Ethernet タイプ（eth で固定です）、シャーシ番号、サブスロット番号、インタフェース番号が含まれます。

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: アクセスノードの識別子を指定します。

- **mac**: ノード識別子として MAC アドレスを使用します。
- **sysname**: ノード識別子として装置名を使用します。装置名は system view の **sysname** コマンドを使用して設定することができます。装置名のパディング形式は指定したパディング形式に関わらず、常に ASCII です。
- **user-defined** *node-identifier*: ユーザ定義のノード識別子を使用します。設定範囲は 1～50 です。大文字、小文字を区別します。指定された文字列のパディング形式は指定したパディング形式に関われず、常に ASCII になります。

Interface: インタフェース情報としてインタフェース名を使用します。インタフェース名のパディング形式は、指定したパディング形式に関係なく、常に ASCII です。

format: circuit ID サブオプションのコードタイプを指定します。

ascii: ASCII コードタイプを指定します。

hex: hex のコードタイプを指定します。

説明

dhcp relay information circuit-id コマンドはオプション 82 の circuit ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp relay information circuit-id コマンドはデフォルトに戻します。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

ユーザ定義、normal モード、verbose モードのパディング形式はコマンドの設定によって変わります。表 9-8 に異なるモードのパディング形式を示します。

表 9-7 異なるモードのパディング形式

キーワード（モード）	パディング形式が指定されていない場合	パディング形式が ASCII	パディング形式が hex
string *circuit-id*	パディング形式を指定できません。常にASCIIになります。	ー	ー
normal	hexです。	ASCIIです。	hexです。
verbose	VLAN IDはhexです。 ノード識別子、Ethernetタイプ、インタフェース番号はASCIIです。	ASCIIです。	ノード識別子とEthernetタイプはASCIIです。 インタフェース番号とVLAN IDはhexです。

例

circuit ID サブオプションのコードモードが verbose、ノード識別子が装置名、パディング形式が ASCII に指定します。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] dhcp relay information enable

[AP-Vlan-interface10] dhcp relay information strategy replace

[AP-Vlan-interface10] dhcp relay information circuit-id verbose node-identifier sysname format ascii

関連コマンド

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

9.3.4 dhcp relay information enable

Syntax

dhcp relay information enable

undo dhcp relay information enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

dhcp relay information enable コマンドはリレーエージェントでオプション 82 のサポートを有効にします。

undo dhcp relay information enable コマンドはオプション 82 のサポートを無効にします。

このコマンドによって DHCP リレーエージェントが DHCP サーバに要求を転送する前に、オプション 82 が含まれない DHCP 要求にオプション 82 を追加します。オプション 82 の内容は **dhcp relay information circuit-id** コマンド、**dhcp relay information remote-id** コマンドによって決まります。DHCP 要求にオプション 82 が含まれる場合、リレーエージェントは **dhcp relay information strategy** コマンドで設定された方法にしたがって DHCP 要求を処理します。

この機能が無効である場合、リレーエージェントはオプション 82 を含む DHCP 要求とオプション 82 を含まない DHCP 要求を DHCP サーバに転送します。

例

オプション 82 のサポートを有効にします。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] dhcp relay information enable

関連コマンド

- **dhcp relay information circuit-id**
- **dhcp relay information remote-id**
- **dhcp relay information strategy**
- **display dhcp relay information**

9.3.5 dhcp relay information remote-id

Syntax

dhcp relay information remote-id { { **ap-mac** | **ap-mac-ssid** | **normal** } [**format** { **ascii** | **hex** }] | **ap-name** | **ap-name-ssid** | **string** *remote-id* | **sysname** }

undo dhcp relay information remote-id

デフォルト

コードモードは normal で、パディング形式は hex です。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ap-mac: リモート ID サブオプションに AP の MAC アドレスを埋め込むことを指定します。

ap-mac-ssid: リモート ID サブオプションに AP の MAC アドレスと SSID をコロン (:) で区切って埋め込むことを指定します。SSID の詳細については、はコマンドマニュアルのセクション 5 の *WLAN アクセス "WLAN アクセスの設定"* を参照してください。

normal: コードモードを normal モードに指定します。このパディングの内容は受信インタフェースの MAC アドレスです。

format: remote ID サブオプションのコードタイプを指定します。デフォルトコードタイプは hex です。

ascii: ASCII コードタイプを指定します。

hex: hex のコードタイプを指定します。

ap-name: リモート ID サブオプションに AP の名前をパディングします。AP 名の詳細については、はコマンドマニュアルのセクション 6 *AP 管理 "AP 管理"* を参照してください。

ap-name-ssid: リモート ID サブオプションに AP の名前と SSID をコロン (:) で区切って埋め込むことを指定します。

string *remote-id*: remote ID サブオプションの内容を指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

sysname: リモート ID サブオプションの内容として装置名を指定します。装置名は **sysname** コマンドを使用して設定することができます。

説明

dhcp relay information remote-id コマンドはオプション 82 の remote ID サブオプションのパディング内容とパディング形式を設定します。

undo dhcp relay information remote-id コマンドはデフォルトに戻します。

指定した文字列（**string**）あるいは装置名（**sysname**）は常に ASCII です。normal モードのパディング形式はコマンドの設定によって変わります。

指定された文字列(**string**)、および装置名(**sysname**)は ASCII です。パディングフォーマットはコマンドによって決定されます。

コマンドを複数回設定した場合、最後に行った設定が適用されます。

例

オプション 82 の remote ID サブオプションのパディング内容を device001 に指定します。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] dhcp relay information enable

[AP-Vlan-interface10] dhcp relay information strategy replace

[AP-Vlan-interface10] dhcp relay information remote-id string device001

関連コマンド

- **dhcp relay information enable**
- **dhcp relay information strategy**
- **display dhcp relay information**

9.3.6 dhcp relay information strategy

Syntax

dhcp relay information strategy { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

デフォルト

replace

View

Interface view

定義済みユーザロール

network-admin

パラメータ

drop: オプション 82 メッセージが含まれる DHCP メッセージを廃棄します。

keep: オプション 82 を含むメッセージをそのまま転送するよう指定します。

replace: 元のオプション 82 のメッセージを設定されたオプション 82 のメッセージに置き換えします。

説明

dhcp relay information strategy コマンドはDHCP リレーエージェントでオプション82が含まれるメッセージの処理方法を設定します。

undo dhcp relay information strategy コマンドはデフォルトに戻します。

このコマンドは DHCP 要求にオプション 82 が含まれるときのみ適用します。

DHCP 要求にオプション 82 が含まれない場合、DHCP リレーエージェントは DHCP サーバに DHCP 要求を転送する前、常に DHCP 要求にオプション 82 を追加します。

replace パラメータを指定した場合、オプション 82 のパディングモード、パディング形式を設定してください。

keep パラメータあるいは **drop** パラメータを指定した場合､オプション 82 のパディングモード、パディング形式を設定する必要はありません。設定しても適用されません。

例

DHCP リレーエージェントでオプション 82 が含まれるメッセージの処理方法を keep に設定します。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] dhcp relay information enable

[AP-Vlan-interface10] dhcp relay information strategy keep

関連コマンド

- **dhcp relay information enable**
- **display dhcp relay information**

9.3.7 dhcp relay release ip

Syntax

dhcp relay release ip *ip-address*

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: リリースされる IP アドレスを指定します。

説明

dhcp relay release ip コマンドは指定したクライアントの IP アドレスをリリースします。

このコマンドを実行した後、リレーエージェントは DHCP サーバに DHCP-RELEASE パケットを送信し、IP アドレスのリレーエントリを削除します。パケットを受信するとサーバは、IP アドレスをリリースするため、指定された IP アドレスの割り当て情報を削除します。

例

IP アドレス 1.1.1.1 をリリースします。

<AP> system-view

[AP] dhcp relay release ip 1.1.1.1

9.3.8 dhcp relay server-address

Syntax

dhcp relay server-address *ip-address*

undo dhcp relay server-address [*ip-address*]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ip-address: DHCP サーバの IP アドレスを指定します。DHCP リレーエージェントは DHCP クライアントから受信した DHCP パケットを DHCP サーバに転送します。

説明

dhcp relay server-address コマンドは DHCP リレーエージェントの DHCP サーバを指定します。

undo dhcp relay server-address コマンドは DHCP サーバを削除します。

DHCP サーバを指定する IP アドレスは、DHCP リレーエージェントインタフェースの IP アドレスと同一のサブネット上にすることはできません。そうでなければ、DHCP クライアントは IP アドレスの取得に失敗します。

インタフェースで最大 8 つの DHCP サーバを指定することができます。DHCP リレーエージェントはクライアントからのパケットをすべての指定された DHCP サーバに転送します。

IP アドレスを指定しない場合、**undo dhcp relay server-address** コマンドはインタフェースのすべての DHCP サーバを削除します。

例

リレーエージェントの VLAN インタフェース 10 で DHCP サーバ 1.1.1.1 を指定します。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] dhcp relay server-address 1.1.1.1

関連コマンド

- **dhcp select relay**

- **display dhcp relay interface**

9.3.9 display dhcp relay client-information

Syntax

display dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースのリレーエントリを表示します。指定しない場合、リレーエージェントのすべてのインタフェースのリレーエントリを表示します。

ip *ip-address*: 指定された IP アドレスのリレーエントリを表示します。指定しない場合、リレーエージェントのすべての IP アドレスのリレーエントリを表示します。

説明

display dhcp relay client-information コマンドはリレーエージェントのリレーエントリを表示します。

dhcp relay client-information record コマンドが設定されているときのみ、DHCP リレーエージェントはリレーエントリを記録します。

例

リレーエージェントのすべてのリレーエントリを表示します。

<AP> display dhcp relay client-information

```
Total number of client-information items: 2
Total number of dynamic items: 1
Total number of temporary items: 1
IP address      MAC address     Type       Interface          VPN name
10.1.1.5        00e0-0000-0000  Temporary  Vlan2              N/A
```

表 9-8 コマンド出力

フィールド	説明
Total number of client-information items	リレーエントリの総数です。
Total number of dynamic items	ダイナミックリレーエントリの総数です。
Total number of temporary items	一時的なリレーエントリの総数です。
IP address	DHCPクライアントのIPアドレスです。
MAC address	DHCPクライアントのMACアドレスです。
Type	リレーエントリタイプです。 • **Dynamic**—リレーエージェントはDHCPサーバからAck応答を受信した際にダイナミックリレーエントリを作成します。 • **Temporary**—リレーエージェントはDHCPクライアントらREQUESTパケットを受信した際に一時的なリレーエントリを作成します。
Interface	DHCPクライアントに接続されたレイヤ3インタフェースです。リレーエージェントにインタフェース情報がない場合、**N/A**と表示されます。
VPN name	DHCPクライアントが所属しているVPNインスタンスの名前です。DHCPクライアントがVPNに所属していない場合、**N/A**と表示されます。

関連コマンド

- **dhcp relay client-information record**
- **reset dhcp relay client-information**

9.3.10 display dhcp relay information

Syntax

display dhcp relay information [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースのオプション 82 の設定情報を表示します。インタフェースを指定しない場合、すべてのインタフェースのオプション 82 の設定情報を表示します。

説明

display dhcp relay information コマンドは DHCP リレーエージェントのオプション 82 の設定情報を表示します。

例

すべてのインタフェースのオプション 82 の設定情報を表示します。

<AP> display dhcp relay information

```
Interface: Vlan-interface100
  Status: Enable
  Strategy: Replace
  Circuit ID Pattern: Verbose
  Remote ID Pattern: Sysname
  Circuit ID format-type: Undefined
  Remote ID format-type: ASCII
  Node identifier: aabbcc
Interface: Vlan-interface200
  Status: Enable
  Strategy: Replace
  Circuit ID Pattern: User Defined
  Remote ID Pattern: User Defined
  Circuit ID format-type: ASCII
  Remote ID format-type: ASCII
  User defined:
  Circuit ID: vlan100
  Remote ID: device001
```

表 9-9 コマンド出力

フィールド	説明
Interface	インタフェース名です。
Status	オプション82の状態です。 ● **Enable**—DHCPリレーエージェントはオプション82のサポートが有効です。 ● **Disable**—DHCPリレーエージェントはオプション82のサポートが無効です。
Strategy	要求メッセージの処理方法です。 **Option 82**、**Drop**、**Keep**、**Replace**が含まれます。
Circuit ID Pattern	circuit IDサブオプションのパディングモードです。**Verbose**、**Normal**、**User Defined**があります。
Remote ID Pattern	remote IDサブオプションのパディングモードです。**Sysname**、**Normal**、**User Defined**があります。
Circuit ID format-type	circuit IDサブオプションのパディング形式です。**ASCII**、**Hex**、**Undefined**があります。
Remote ID format-type	remote IDサブオプションのパディング形式です。**ASCII**、**Hex**、**Undefined**があります。
Node identifier	アクセスノード識別子です。
User defined	ユーザ定義サブオプションの内容です。
Circuit ID	circuit IDサブオプションのユーザ定義の内容です。
Remote ID	remote IDサブオプションのユーザ定義の内容です。

9.3.11 display dhcp relay server-address

Syntax

display dhcp relay server-address [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースの DHCP サーバのアドレスを表示します。指定しない場合、DHCP リレーエージェントで動作するすべてのインタフェースの DHCP サーバのアドレスを表示します。

説明

display dhcp relay server-address コマンドはインタフェースに設定された DHCP サーバのアドレスを表示します。

例

すべてのインタフェースの DHCP サーバのアドレスを表示します。

<AP> display dhcp relay server-address

```
Interface name              Server IP address
Vlan2                       2.2.2.2
```

表 9-10 コマンド出力

フィールド	説明
Interface name	インタフェース名です。
Server IP address	DHCPサーバのIPアドレスです。

関連コマンド

dhcp relay server-address

9.3.12 display dhcp relay statistics

Syntax

display dhcp relay statistics [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 指定したインタフェースの DHCP パケットの統計情報を表示します。指定しない場合、DHCP リレーエージェントのすべての DHCP パケットの統計情報を表示します。

説明

display dhcp relay statistics コマンドは DHCP リレーエージェントの DHCP パケットの統計情報を表示します。

例

DHCP リレーエージェントのすべての DHCP パケットの統計情報を表示します。

<AP> display dhcp relay statistics

```
DHCP packets dropped:               0
DHCP packets received from clients:   0
   DHCPDISCOVER:                    0
   DHCPREQUEST:                     0
   DHCPINFORM:                      0
   DHCPRELEASE:                     0
   DHCPDECLINE:                     0
   BOOTPREQUEST:                    0
DHCP packets received from servers:   0
   DHCPOFFER:                       0
   DHCPACK:                         0
   DHCPNAK:                         0
   BOOTPREPLY:                      0
DHCP packets relayed to servers:      0
   DHCPDISCOVER:                    0
   DHCPREQUEST:                     0
   DHCPINFORM:                      0
   DHCPRELEASE:                     0
```

```
  DHCPDECLINE:                    0
  BOOTPREQUEST:                   0
DHCP packets relayed to clients:      0
  DHCPOFFER:                      0
  DHCPACK:                        0
  DHCPNAK:                        0
  BOOTPREPLY:                     0
DHCP packets sent to servers:         0
  DHCPDISCOVER:                   0
  DHCPREQUEST:                    0
  DHCPINFORM:                     0
  DHCPRELEASE:                    0
  DHCPDECLINE:                    0
  BOOTPREQUEST:                   0
DHCP packets sent to clients:         0
  DHCPOFFER:                      0
  DHCPACK:                        0
  DHCPNAK:                        0
  BOOTPREPLY:                     0
```

関連コマンド

reset dhcp relay statistics

9.3.13 reset dhcp relay client-information

Syntax

reset dhcp relay client-information [**interface** *interface-type interface-number* | **ip** *ip-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースのリレーエントリを削除します。指定しない場合、すべてのインタフェースのリレーエントリを削除します。

ip *ip-address*: 指定された IP アドレスのリレーエントリを削除します。指定しない場合、すべての IP アドレスのリレーエントリを削除します。

説明

reset dhcp relay client-information コマンドは DHCP リレーエージェントのリレーエントリを削除します。

例

DHCP リレーエージェントのすべてのリレーエントリを削除します。

<AP> reset dhcp relay client-information

関連コマンド

display dhcp relay client-information

9.3.14 reset dhcp relay statistics

Syntax

reset dhcp relay statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 指定されたインタフェースの DHCP リレーエージェントの統計情報を削除します。指定しない場合、すべての DHCP リレーエージェントの統計情報を削除します。

説明

reset dhcp relay statistics コマンドは DHCP リレーエージェントの統計情報を削除します。

例

すべての DHCP リレーエージェントの統計情報を削除します。

<AP> reset dhcp relay statistics

関連コマンド

display dhcp relay statistics

9.4 DHCP クライアント設定コマンド

9.4.1 dhcp client dad enable

Syntax

dhcp client dad enable

undo dhcp client dad enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

dhcp client dad enable コマンドはアドレス重複の検出を有効にします。

undo dhcp client dad enable コマンドはアドレス重複の検出を無効にします。

DHCP クライアントは、ARP パケットを使用して IP アドレスの重複があるかどうかを検出します。攻撃者は、サーバが割り当てた IP アドレスを使用できなくさせるため、ARP 応答を送信し、IP アドレスのオーナーとして動作します。ARP 攻撃がネットワークに存在する場合、アドレス重複検出機能を無効にすることを推奨します。

例

アドレス重複の検出を無効にします。

<AP> system-view

[AP] undo dhcp client dad enable

9.4.2 dhcp client dscp

Syntax

dhcp client dscp *dscp-value*

undo dhcp client dscp

デフォルト

56

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DHCP パケットの DSCP を設定します。設定範囲は 0〜63 です。

説明

dhcp client dscp コマンドはDHCP クライアントによって送信されるDHCP パケットの DSCP を設定します。

undo dhcp client dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

DHCP クライアントによって送信されるDHCP パケットのDSCP を30 に設定します。

<AP> system-view

[AP] dhcp client dscp 30

9.4.3 display dhcp client

Syntax

display dhcp client [**verbose**] [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: DHCP クライアントの詳細情報を表示します。指定しない場合、DHCP クライアントの概要情報を表示します。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの DHCP クライアントの情報を表示します。

説明

display dhcp client コマンドは DHCP クライアントの情報を表示します。

例

すべてのインタフェースの DHCP クライアントの情報を表示します。

<AP> display dhcp client

```
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

インタフェースの DHCP クライアントの詳細情報を表示します。

<AP> display dhcp client verbose

```
Vlan-interface10 DHCP client information:
 Current state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from May 21 19:00:29 2012   to   May 31 19:00:29 2012
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
 Classless static routes:
   Destination: 1.1.0.1, Mask: 255.0.0.0, NextHop: 192.168.40.16
   Destination: 10.198.122.63, Mask: 255.255.255.255, NextHop: 192.168.40.16
 DNS servers: 44.1.1.11 44.1.1.12
 Domain name: ddd.com
 Boot servers: 200.200.200.200  1.1.1.1
 ACS parameter:
   URL: http://192.168.1.1:7547/acs
   Username: bims
   Password: ******
```

```
Client ID type: acsii(type value=00)
Client ID value: 000c.29d3.8659-Vlan10
Client ID (with type) hex: 0030-3030-632e-3239-
                      6433-2e38-3635-392d-
                      4574-6830-2f30-2f32
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

表 9-11 コマンド出力

フィールド	説明
DHCP client information	DHCPクライアントを提供するインタフェースの情報です。
Current state	DHCPクライアントの現在の状態です。 • **HALT**—クライアントがIPサービスの適用を停止します。 • **INIT**—初期化状態です。 • **SELECTING**—クライアントがDHCPサーバを検索するため、DHCP-DISCOVERメッセージを送信し、DHCPサーバからの応答を待っています。 • **REQUESTING**—クライアントがIPアドレスを要求するDHCP-REQUESTメッセージを送信し、DHCPサーバからの応答を待っています。 • **BOUND**—クライアントがDHCPサーバからDHCP-ACKメッセージを受信し、正常にIPアドレスを受信しました。 • **RENEWING**—T1タイマがタイムアウトしました。 • **REBOUNDING**— T2タイマがタイムアウトしました。
Allocated IP	DHCPサーバによって割り当てられたIPアドレスです。
Allocated lease	割り当てられたリース時間です。
T1	DHCPクライアントのIPアドレスの1/2リース時間です。単位は秒です。
T2	DHCPクライアントのIPアドレスの7/8リース時間です。単位は秒です。
Lease from….to….	リース開始時間と終了時間です。
DHCP server	IPアドレスを割り当てたDHCPサーバのIPアドレスです。
Transaction ID	トランザクションIDです。IPアドレスの割り当てを特定するために、クライアントがランダムに選択する番号です。
Default router	クライアントに割り当てられるゲートウェイアドレスです。
Classless static routes	クライアントに割り当てられるクラスレススタティックルートです。

フィールド	説明
Static routes	クライアントに割り当てられるクラスフルスタティックルートです。
DNS servers	クライアントに割り当てられるDHCPサーバのアドレスです。
Domain name	クライアントに割り当てられるドメイン名サフィックスです。
Boot servers	DHCPクライアント用に指定されるPXEサーバアドレスです（最大16アドレス）。オプション43によって取得されます。
ACS parameter	ACSのパラメータです。
URL	ACSのURLです。
Username	ACSにログインするユーザ名です。
Password	ACSにログインするパスワードです。パスワードが設定されている場合、******と表示されます。パスワードが設定されていない場合、表示されません。
Client ID type	DHCPクライアントIDタイプです。 • クライアントIDとしてASCIIが使用されている場合、タイプの値は00です。 • クライアントIDとして指定したインタフェースのMACアドレスが使用されている場合、タイプの値は01です。 • クライアントIDとしてhexが使用されている場合、タイプの値は文字列の最初の2文字です。
Client ID value	DHCPクライアントIDの値です。
Client ID (with type) hex	タイプフィールドによるクライアントIDです。16進数の文字列です。
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	T1タイマ（1/2リース時間）がタイムアウトする時間です。

関連コマンド

ip address dhcp-alloc

9.4.4 ip address dhcp-alloc

Syntax

ip address dhcp-alloc

undo ip address dhcp-alloc

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

説明

ip address dhcp-alloc コマンドは DHCP を使用して IP アドレスを取得するインタフェースを設定します。

undo ip address dhcp-alloc コマンドはインタフェースで DHCP の使用を停止します。

undo ip address dhcp-alloc コマンドを実行したとき、インタフェースは DHCP を通して取得した IP アドレスをリリースするため、DHCP-RELEASE メッセージを送信します。インタフェースがダウンしている場合、メッセージを送信することができません。

例

DHCP を使用して IP アドレスを取得する VLAN インタフェース 10 を設定します。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] ip address dhcp-alloc

関連コマンド

display dhcp client

9.5 BOOTPクライアント設定コマンド

9.5.1 display bootp client

Syntax

display bootp client [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの BOOTP クライアント情報を表示します。

説明

display bootp client コマンドは BOOTP クライアントの情報を表示します。

例

VLAN インタフェース 10 の BOOTP クライアントの情報を表示します。

<AP> display bootp client interface vlan-interface 10

```
Vlan-interface10 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID: 0x3d8a7431
MAC Address: 7455-c8fd-c180
```

表 9-12 コマンド出力

フィールド	説明
BOOTP client information	BOOTPクライアントとして動作するインタフェースの情報です。
Allocated IP	BOOTPサーバによって割り当てられたBOOTPクライアントのIPアドレスです。
Transaction ID	BOOTPメッセージの**XID**フィールドの値です。BOOTPクライアントがBOOTPサーバにBOOTP要求を送信するときにランダムに選択される番号です。この値はBOOTPサーバからの応答メッセージを一致させるために使用します。 BOOTP応答とBOOTP要求の**XID**フィールドの値が異なる場合、BOOTPクライアントはBOOTP応答を廃棄します。

フィールド	説明
Mac Address	BOOTPクライアントのMACアドレスです。

関連コマンド

ip address bootp-alloc

9.5.2 ip address bootp-alloc

Syntax

ip address bootp-alloc

undo ip address bootp-alloc

デフォルト

IP アドレスを取得するためインタフェースは BOOTP を使用しません。

View

Interface view

定義済みユーザロール

network-admin

説明

ip address bootp-alloc コマンドは IP アドレスを取得するために BOOTP を使用するインタフェースを設定します。

undo ip address bootp-alloc コマンドはインタフェースで BOOTP を使用することを中止します。

例

IP アドレスを取得するために BOOTP を使用する VLAN インタフェース 10 を設定します。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] ip address bootp-alloc

関連コマンド

display bootp client

目次

このセクションのページは **4-x-x** です。

10 章 DNS 10-1
10.1 DNS 設定コマンド 10-1
10.1.1 display dns domain 10-1
10.1.2 display dns host 10-3
10.1.3 display dns server 10-5
10.1.4 dns domain 10-6
10.1.5 dns dscp 10-7
10.1.6 dns proxy enable 10-7
10.1.7 dns server 10-8
10.1.8 ip host 10-9
10.1.9 reset dns host 10-10

10章 DNS

10.1 DNS設定コマンド

10.1.1 display dns domain

Syntax

display dns domain [**dynamic**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: DHCP または他のプロトコルによってダイナミックに取得したドメイン名のサフィックスを表示します。指定しない場合、スタティックに設定したドメイン名のサフィックスおよび、ダイナミックに取得したドメイン名のサフィックスを表示します。

説明

display dns domain コマンドはドメイン名のサフィックスを表示します。

例

パブリックネットワークのドメイン名のサフィックスを表示します。

<AP> display dns domain

```
Type:
  D: Dynamic    S: Static

No.    Type   Domain suffix
1      S      com
2      D      net
```

表 10-1 コマンド出力

フィールド	説明
No.	シーケンス番号です。
Type	ドメイン名のサフィックスのタイプです。 • **S**—スタティックに設定されたドメイン名のサフィックスです。 • **D**—DHCPまたは他のプロトコルによってダイナミックに取得したドメイン名のサフィックスです。
Domain suffix	ドメイン名のサフィックスです。

関連コマンド

dns domain

10.1.2 display dns host

Syntax

display dns host [**ip**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip: タイプ A のクエリを指定します。タイプ A のクエリは IPv4 アドレスにドメイン名サフィックスをマッピングします。

説明

display dns host コマンドはドメイン名－IP アドレスのマッピングを表示します。

パラメータを指定しない場合、すべてのクエリタイプのドメイン名－IP アドレスのマッピングを表示します。

例

すべてのクエリタイプのドメイン名－IP アドレスのマッピングを表示します。

<AP> display dns host

```
Type:
  D: Dynamic    S: Static

Total number: 3
No.  Host name        Type  TTL       Query type   IP addresses
1    sample.com       D     3132       A           192.168.10.1
                                                    192.168.10.2
                                                    192.168.10.3
2    zig.sample.com    S    -         A            192.168.1.1
3    sample.net        S    -         AAAA         FE80::4904:4448
```

表 10-2 コマンド出力

フィールド	説明
No.	シーケンス番号です。
Host name	ドメイン名です。

フィールド	説明
Interface	出力するインタフェースの名前です。
Type	ドメイン名ーIPアドレスマッピングのタイプです。 • **S—ip host**コマンドで設定されたスタティックマッピングです。 • **D**—ダイナミックドメイン名解決によってダイナミックに取得したマッピングです。
TTL	マッピングがキャッシュに記録できる時間です。単位は秒です。 スタティックマッピングの場合、ハイフン（-）が表示されます。
Query type	クエリタイプです。タイプA、タイプAAAAがあります。
IP addresses	応答したIPアドレスです。 • タイプAクエリでは、応答したIPアドレスはIPv4アドレスです。

関連コマンド

- **ip host**
- **reset dns host**

10.1.3 display dns server

Syntax

display dns server [**dynamic**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: DHCP あるいは他のプロトコルによってダイナミックに取得した IPv4 DNS サーバの情報です。指定しない場合、スタティックに設定された IPv4 DNS サーバとダイナミックに取得した IPv4 DNS サーバを表示します。

説明

display dns server コマンドは IPv4 DNS サーバの情報を表示します。

例

パブリックネットワークの IPv4 DNS サーバの情報を表示します。

<AP> display dns server

```
Type:
  D: Dynamic    S: Static

No. Type  IP address
1   S     202.114.0.124
2   S     169.254.65.125
```

表 10-3 コマンド出力

フィールド	説明
No.	シーケンス番号です。
Type	DNSサーバタイプです。 • **S**—スタティックに設定されたDNSサーバの情報です。 • **D**—DHCPあるいは他のプロトコルによってダイナミックに取得したDNSサーバの情報です。
IP address	DNSサーバのIPv4アドレスです。

関連コマンド

dns server

10.1.4 dns domain

Syntax

dns domain *domain-name*

undo dns domain *domain-name*

デフォルト

ドメイン名サフィックスは設定されていません。既定のドメイン名のみが解決できます。

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名サフィックスを指定します。ドメイン名サフィックスは、ドットにより区切られた文字列により構成されます。ドメイン名サフィックスは、大文字、小文字を区別しない文字、数字、ハイフン（-）、アンダーバー（_）、ドット（.）を使用することができます。たとえば、aabbcc.com です。合計の文字数は 253 文字までです。それぞれの区切られた文字列は 63 文字までです。

説明

dns domain コマンドはドメイン名サフィックスを設定します。

undo dns domain コマンドは指定されたドメイン名サフィックスを削除します。

システムはホスト解決を行うため、ホストから受信したドメイン名の順番でサフィックスを自動で追加します。

パブリックネットワークで最大 16 のドメイン名サフィックスを指定することができます。

例

パブリックネットワークのドメイン名サフィックスを設定します。

<AP> system-view

[AP] dns domain com

関連コマンド

display dns domain

10.1.5 dns dscp

Syntax

dns dscp *dscp-value*

undo dns dscp

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: DSCP を指定します。設定範囲は 0〜63 です。

説明

dns dscp コマンドは DNS クライアントあるいは DNS Proxy によって送信された DNS パケットの DSCP を設定します。

undo dns dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。DSCP の値が大きくなると、プライオリティが高くなります。

例

送信 DNS パケットの DSCP を 30 に設定します。

<AP> system-view

[AP] dns dscp 30

10.1.6 dns proxy enable

Syntax

dns proxy enable

undo dns proxy enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dns proxy enable コマンドは DNS Proxy を有効にします。

undo dns proxy enable コマンドは DNS Proxy を無効にします。

例

DNS Proxy を有効にします。

<AP> system-view

[AP] dns proxy enable

10.1.7 dns server

Syntax

dns server *ip-address*

undo dns server [*ip-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: DNS サーバの IPv4 アドレスを指定します。

説明

dns server コマンドは DNS サーバの IPv4 アドレスを指定します。

undo dns server コマンドは DNS サーバの IPv4 アドレスを削除します。

装置は IPv4 アドレスが指定された順番で、DNS サーバに DNS クエリ要求を送信します。

パブリックネットワークで最大 6 つの DNS サーバの IPv4 アドレスを指定することができます。

IPv4 アドレスを指定しない場合、**undo dns server** コマンドはパブリックネットワークのすべての DNS サーバの IPv4 アドレスを削除します。

例

DNS サーバの IPv4 アドレス 172.16.1.1 を指定します。

<AP> system-view

[AP] dns server 172.16.1.1

関連コマンド

display dns server

10.1.8 ip host

Syntax

ip host *host-name ip-address*

undo ip host *host-name ip-address*

デフォルト

ホスト名と IPv4 アドレスのマッピングは存在しません。

View

System view

定義済みユーザロール

network-admin

パラメータ

host-name: ホスト名を指定します。設定範囲は 1～253 です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含めることができます。

ip-address: ホストの IPv4 アドレスを指定します。

説明

ip host コマンドはホスト名－IPv4 アドレスマッピングを作成します。

undo ip host コマンドはマッピングを削除します。

最大 1024 のホスト名－IPv4 アドレスマッピングを作成することができます。

パブリックネットワークで各ホスト名は 1 つの IPv4 アドレスのみマッピングすることができます。コマンドを複数回設定した場合、最後に行った設定が適用されます。

ホスト名を使用して **ping** コマンドのパラメータ **ip**、**-a**、**-c**、**-f**、**-h**、**-i**、**-m**、**-n**、**-p**、**-q**、**-r**、**-s**、**-t**、**-tos**、**–v** を実行することができません。**ping** コマンドのパラメータの詳細は

コマンドマニュアルのセクション 15 *ネットワーク管理 とモニタ“システムの保守とデバッグ”*を参照してください。

例

パブリックネットワークの IPv4 アドレス 10.110.0.1 をホスト名 aaa にマッピングします。

<AP> system-view

[AP] ip host aaa 10.110.0.1

関連コマンド

display dns host

10.1.9 reset dns host

Syntax

reset dns host [**ip**]

View

User view

定義済みユーザロール

network-admin

パラメータ

ip: タイプ A のクエリを指定します。タイプ A のクエリは IPv4 アドレスにドメイン名サフィックスをマッピングします。

説明

reset dns host コマンドはダイナミック DNS キャッシュの情報を削除します。

パラメータを指定しない場合、すべてのクエリタイプのダイナミック DNS キャッシュ情報を削除します。

例

パブリックネットワークのすべてのクエリタイプのダイナミック DNS キャッシュ情報を削除します。

<AP> reset dns host

関連コマンド

display dns host

目次

このセクションのページは **4-x-x** です。

11 章 NAT 11-1
11.1 NAT コマンド 11-1
11.1.1 address 11-1
11.1.2 display nat address-group 11-2
11.1.3 display nat alg 11-5
11.1.4 display nat all 11-6
11.1.5 display nat eim 11-10
11.1.6 display nat inbound 11-12
11.1.7 display nat log 11-14
11.1.8 display nat no-pat 11-16
11.1.9 display nat outbound 11-17
11.1.10 display nat session 11-19
11.1.11 display nat static 11-22
11.1.12 display nat statistics 11-26
11.1.13 nat address-group 11-28
11.1.14 nat alg 11-29
11.1.15 nat icmp-error reply 11-30
11.1.16 nat inbound 11-32
11.1.17 nat inbound rule move 11-35
11.1.18 nat log alarm 11-36
11.1.19 nat log enable 11-37
11.1.20 nat log flow-active 11-39
11.1.21 nat log flow-begin 11-40
11.1.22 nat log flow-end 11-41
11.1.23 nat mapping-behavior endpoint-independent 11-41
11.1.24 nat outbound 11-44
11.1.25 nat outbound rule move 11-47
11.1.26 nat static enable 11-48
11.1.27 nat static inbound 11-50
11.1.28 nat static inbound net-to-net 11-53
11.1.29 nat static inbound rule move 11-55
11.1.30 nat static outbound 11-57
11.1.31 nat static outbound net-to-net 11-60
11.1.32 nat static outbound rule move 11-62
11.1.33 reset nat count statistics 11-63
11.1.34 reset nat session 11-65

11章 NAT

11.1 NATコマンド

11.1.1 address

Syntax

address *start-address end-address*

undo address *start-address end-address*

デフォルト

設定なし

View

NAT address group view

定義済みユーザロール

network-admin

パラメータ

start-address end-address: アドレス範囲の開始 IP アドレスと終了 IP アドレスを指定します。終了アドレスは開始アドレスより小さくできません。同じ場合、アドレス範囲には IP アドレスが 1 つしかありません。IP アドレスの範囲は 65535 個まで指定できます。

説明

address コマンドは NAT アドレスグループにアドレス範囲を追加します。

undo address コマンドは NAT アドレスグループからアドレス範囲を削除します。

NAT アドレスグループは、アドレス範囲のセットです。外部ネットワーク宛てのパケットの送信元アドレスは、アドレス範囲の 1 つのアドレスに変換されます。

単一の NAT アドレスグループまたは複数の NAT アドレスグループのアドレス範囲が重複していないことを確認します。

例

#アドレスグループにアドレス範囲を追加します。

<AP> system-view

[AP] nat address-group 2

[AP-address-group-2] address 10.1.1.1 10.1.1.15

[AP-address-group-2] address 10.1.1.20 10.1.1.30

関連コマンド

nat address-group

11.1.2 display nat address-group

Syntax

display nat address-group [*group-id*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-id: NAT アドレスグループの ID を指定します。この値の範囲は 0 から 65535 です。*group-id* 引数を指定しない場合、このコマンドはすべての NAT アドレスグループに関する情報を表示します。

説明

display nat address-group コマンドは NAT アドレスグループ情報を表示します。

例

すべての NAT アドレスグループに関する情報を表示します。

<AP> display nat address-group

```
NAT address group information:
  Totally 5 NAT address groups.
  Address group ID: 1    Address group name: a
    Port range: 1-65535
    Address information:
      Start address        End address
      202.110.10.10        202.110.10.15

  Address group ID: 2
    Port range: 1-65535
    Address information:
      Start address        End address
      202.110.10.20        202.110.10.25
      202.110.10.30        202.110.10.35
```

```
Address group ID: 3
  Port range: 1024-65535
  Address information:
    Start address        End address
    202.110.10.40        202.110.10.50

Address group ID: 4
  Port range: 10001-65535
  Address information:
    Start address        End address
    202.110.10.60        202.110.10.65

Address group ID: 6
  Port range: 1-65535
  Address information:
    Start address        End address
    ---                 ---
```

#NAT アドレスグループ 1 に関する情報を表示します。

<AP> display nat address-group 1

```
Address group ID: 1    Address group name: a
  Port range: 1-65535
  Address information:
    Start address        End address
    202.110.10.10        202.110.10.15
```

表 11-1 コマンド出力

フィールド	説明
NAT address group information	NATアドレスグループに関する情報
Address group ID	NATアドレスグループのID。
Totally n NAT address groups	NATアドレスグループの総数。
Address group name	NATアドレスグループの名前。アドレスグループ名が設定されていない場合、このフィールドは表示されません。
Port range	パブリックIPアドレスのポート範囲。

フィールド	説明

Address information	アドレスグループ内のIPアドレスに関する情報。
	• addressコマンドを使用して追加されたアドレスの場合:
	  • Start address :アドレス範囲の開始IPアドレス。範囲の開始アドレスを指定しない場合、このフィールドにはハイフン (---) が表示されます。
	  • End address:アドレス範囲の終了IPアドレス。範囲の終了アドレスを指定しない場合、このフィールドにはハイフン (---) が表示されます。

関連コマンド

nat address-group

11.1.3 display nat alg

Syntax

display nat alg

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat alg コマンドはサポートされているすべてのプロトコルの NAT ALG ステータスを表示します。

例

#サポートされているすべてのプロトコルの NAT ALG ステータスを表示します。

<AP> display nat alg

```
NAT ALG:
  DNS       : Enabled
  FTP       : Disabled
  H323      : Disabled
  ICMP-ERROR : Disabled
  ILS       : Disabled
  MGCP      : Disabled
  NBT       : Disabled
  PPTP      : Disabled
  RTSP      : Disabled
  RSH       : Disabled
  SCCP      : Disabled
  SIP       : Disabled
  SQLNET    : Disabled
  TFTP      : Disabled
  XDMCP     : Disabled
```

関連コマンド

display nat all

11.1.4 display nat all

Syntax

display nat all

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat all コマンドはすべての NAT 設定情報を表示します。

例

すべての NAT 設定情報を表示します。

<AP> display nat all

```
NAT address group information:
  Totally 5 NAT address groups.
  Address group ID: 1:
    Port range: 1-65535
    Address information:
      Start address        End address
      202.110.10.10        202.110.10.15

  Address group ID: 2:
    Port range: 1-65535
    Address information:
      Start address        End address
      202.110.10.20        202.110.10.25
      202.110.10.30        202.110.10.35

  Address group ID: 3:
    Port range: 1024-65535
    Address information:
      Start address        End address
      202.110.10.40        202.110.10.50

  Address group ID: 4:
    Port range: 10001-65535
    Address information:
```

```
      Start address       End address
      202.110.10.60       202.110.10.65

  Address group ID: 6:
    Port range: 1-65535
    Address information:
      Start address       End address
      ---                 ---

NAT inbound information:
  Totally 1 NAT inbound rules.
  Interface: Vlan-interface20
    ACL: 2038
    Address group ID: 2
    Add route: Y       NO-PAT:Y  Reversible: N
    Rule name: abc
    Priority: 1000
    NAT counting: 0
    Config status: Active

NAT outbound information:
  Totally 2 NAT outbound rules.
  Interface: Vlan-interface10
    ACL: 2036
    Address group ID: 1
    Port-preserved: Y       NO-PAT: N  Reversible: N
    Rule name: lee
    Priority: 122
    NAT counting: 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

  Interface: Vlan-interface10
    ACL: 2037
    Address group ID: 1
    Port-preserved: N       NO-PAT: Y  Reversible: Y
    Rule name: rabbit
    Priority: 100
    NAT counting: 0
      The following items don't exist or aren't effective: ACL.

Static NAT mappings:
```

```
Totally 2 inbound static NAT mappings.
Net-to-net:
  Global IP    : 2.2.2.1 – 2.2.2.255
  Local IP     : 1.1.1.0
  Netmask      : 255.255.255.0
  ACL         : 3000
  Reversible   : Y
  Rule name    : green
  Priority     : 4
  NAT counting : 0
  Config status: Active

IP-to-IP:
  Global IP    : 5.5.5.5
  Local IP     : 4.4.4.4
  ACL         : 2001
  Reversible   : Y
  Rule name    : blue
  Priority     : 4
  NAT counting : 0
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: ACL.

Totally 2 outbound static NAT mappings.
Net-to-net:
  Local IP     : 1.1.1.1 - 1.1.1.255
  Global IP    : 2.2.2.0
  Netmask      : 255.255.255.0
  ACL         : 3000
  Reversible   : Y
  Rule name    : yellow
  Priority     : 5
  NAT counting : 0
  Config status: Active

IP-to-IP:
  Local IP     : 4.4.4.4
  Global IP    : 5.5.5.5
  ACL:        : 2001
  Reversible   : Y
  Rule name    : pink
  Priority     : 6
```

```
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.

Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active

NAT logging:
  Log enable         : Enabled(ACL 2000)
  Flow-begin         : Disabled
  Flow-end           : Disabled
  Flow-active        : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm              : Disabled
  NO-PAT IP usage     : Disabled

NAT mapping behavior:
  Mapping mode : Endpoint-Independent
  ACL          : 2050
  Config status: Active

NAT ALG:
  DNS       : Enabled
  FTP       : Disabled
  H323      : Enabled
  ICMP-ERROR : Enabled
  ILS       : Enabled
  MGCP      : Enabled
  NBT       : Enabled
  PPTP      : Enabled
  RSH       : Enabled
  RTSP      : Enabled
  SCCP      : Enabled
  SIP       : Disabled
  SQLNET     : Enabled
  TFTP      : Enabled
  XDMCP     : Enabled
```

表 11-2 コマンド出力

フィールド	説明
NAT address group information	NATアドレスグループに関する情報。出力の説明については、表 11-1を参照してください。
NAT inbound information:	インバウンドダイナミックNATコンフィグレーション。出力の説明については、表 11-5を参照してください。
NAT outbound information	送信ダイナミックNATの設定。出力の説明については、表 11-9を参照してください。
Static NAT mappings	スタティックNATマッピング。出力の説明は、表 11-17を参照してください。
NAT logging	NATログの設定。出力の説明については、表 11-6を参照してください。
NAT hairpinning	NATヘアピンの設定です。
Totally *n* interfaces enabled NAT hairpinning	NATヘアピンが有効になっているインタフェースの数です。
Interface	NATヘアピン対応インタフェースです。
Rule name	NATルールの名前です。
Priority	NATルールの優先順位です。
Config status	NATヘアピン設定のステータス (アクティブまたは非アクティブ)です 。
Reasons for inactive status	NATヘアピン設定が有効にならない理由です。このフィールドは、**Config**ステータスが**Inactive**の場合に使用できます。
NAT mapping behavior	PATのマッピング動作モード: Endpoint-Independent または Address and Port-Dependent。
ACL	ACL番号または名前。NATにACLが指定されていない場合、このフィールドにはハイフン (---) が表示されます。
Config status	NATマッピング動作設定のステータス (Activeまたは Inactive) 。
Reasons for inactive status	NATマッピング動作の設定が有効にならない理由。このフィールドは、Configステータスが Inactiveの場合に使用できます。
NAT ALG	異なるプロトコルのNAT ALG設定。

11.1.5 display nat eim

Syntax

display nat eim

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat eim コマンドは NAT EIM (Endpoint-Independent Mapping) エントリに関する情報を表示します。

EIM エントリは、PAT が EIM モードで動作しているときに作成されます。EIM エントリは 3 タプルのエントリで、プライベートアドレス/ポートとパブリックアドレス/ポート間のマッピングを記録します。

EIM エントリには、次の機能があります。

- 同じ送信元 IP およびポートから開始される後続の接続には、同じ EIM エントリが適用されます。
- EIM エントリを使用すると、外部ホストから内部ホストへの接続を逆変換できます。

例

NAT EIM エントリに関する情報を表示します。

<AP> display nat eim

```
Slot 0:
Local  IP/port: 192.168.100.100/1024
Global IP/port: 200.100.1.100/2048
Protocol: TCP(6)

Local  IP/port: 192.168.100.200/2048
Global IP/port: 200.100.1.200/4096
Protocol: UDP(17)

Total entries found: 2
```

表 11-3 コマンド出力

フィールド	説明
Protocol	プロトコルの名前と番号。
Total entries found	EIMエントリの合計数。

関連コマンド

- **nat mapping-behavior**

- **nat outbound**

11.1.6 display nat inbound

Syntax

display nat inbound

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat inbound コマンドは受信ダイナミック NAT に関する設定を表示します。

例

インバウンドダイナミック NAT コンフィグレーションを表示します。

<AP> display nat inbound

```
NAT inbound information:
  Totally 2 NAT inbound rules.
  Interface: Vlan-interface20
    ACL: 2038
    Address group ID: 2
    Add route: Y         NO-PAT: Y  Reversible: N
    Rule name: abcd
    Priority: 1000
    NAT counting: 0
    Config status: Active
```

表 11-4 コマンド出力

フィールド	説明
NAT inbound information	インバウンドダイナミックNAT設定に関する情報。
Totally n NAT inbound rules	インバウンドダイナミックNATルールの合計数。
Interface	受信ダイナミックNATルールが設定されているインタフェース。

フィールド	説明
ACL	ACL番号または名前。
Address group ID	受信ダイナミックNATルールで使用されるNATアドレスグループのID。
Address group name	NATアドレスグループの名前。アドレスグループ名が設定されていない場合、このフィールドは表示されません。
Add route	パケットがインバウンドダイナミックNATルールと一致したときにルートを追加するかどうか。 ・　Y:ルートを追加します。 ・　N:ルートを追加しません。
NO-PAT	NO-PATまたはPATが使用されているかどうか。 ・　Y:NO-PATが使用されます。 ・　N:PATが使用されます。
Reversible	逆アドレス変換が許可されているかどうか。 ・　Y:逆アドレス変換が許可されます。 ・　N:逆アドレス変換は許可されません。
Rule name	NATルールの名前。
Priority	NATルールのプライオリティ。
Description	NATルールの説明です。ルールの説明が設定されていない場合、このフィールドは表示されません。
NAT counting	NATルールが一致した回数。
Config status	受信ダイナミックNATルールのステータス（Activeまたは Inactive）。
Reasons for inactive status	インバウンドダイナミックNATルールが有効にならない理由: このフィールドは、Configステータスが Inactiveの場合に使用できます。

関連コマンド

nat inbound

11.1.7 display nat log

Syntax

display nat log

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat log コマンドは NAT のログ設定を表示します

例

NAT ログ設定を表示します。

<AP> display nat log

```
NAT logging:
  Log enable         : Enabled(ACL 2000)
  Flow-begin         : Disabled
  Flow-end           : Disabled
  Flow-active        : Enabled(10 minutes)
  Port-block-assign   : Disabled
  Port-block-withdraw : Disabled
  Alarm              : Disabled
```

表 11-5 コマンド出力

フィールド	説明
NAT logging	NATログの設定。
Log enable	NATログのステータスを有効にします。 NATログにACLが指定されている場合、このフィールドにはACLの番号または名前も表示されます。
Flow-begin	NATセッション確立イベントのログのステータスを有効にします。
Flow-end	NATセッション削除イベントのログのステータスを有効にします。

フィールド	説明
Flow-active	アクティブなNATフローのログステータスを有効にします。有効の場合、このフィールドにはアクティブフローログが生成される間隔 (分単位) も表示されます。
Port-block-assign	ポートブロック割り当てのNAT 444ユーザーログのステータスを有効にします。
Port-block-withdraw	ポートブロック取り消しのためのNAT 444ユーザーログのステータスを有効にします。
Alarm	NAT 444アラームのログ記録ステータスを有効にします。
NO-PAT IP usage	NO-PATモードを使用している場合の、NATアドレスグループのIP使用状況のログ記録ステータスの有効化。有効になっている場合、このフィールドには、設定されている各NATアドレスグループのIP使用状況もパーセンテージで表示されます。

関連コマンド

- **nat log enable**
- **nat log flow-active**
- **nat log flow-begin**

11.1.8 display nat no-pat

Syntax

display nat no-pat { **ipv4** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv 4: IPv 4 NAT セッションの NO-PAT エントリ情報を表示します。

説明

display nat no-pat コマンドは AT NO-PAT エントリに関する情報を表示します。

NO-PAT エントリは、プライベートアドレスとパブリックアドレス間のマッピングを記録します。

NO-PAT エントリは、次の機能を提供します。

- 同じ送信元 IP アドレスから開始される後続の接続には、同じエントリが適用されます。
- NO-PAT エントリを使用すると、外部ホストから内部ホストへの接続を逆変換できます。

送信および受信 NO-PAT アドレス変換では、独自の NO-PAT テーブルが作成されます。この 2 種類のテーブルは別々に表示されます。

例

すべてのカードの IPv 4 NAT セッションの NO-PAT エントリに関する情報を表示します。

<AP> display nat no-pat ipv4

```
Slot 0:
Global    IPv4: 200.100.1.100
Local      IPv4: 192.168.100.100
Reversible    : N
Type          : Inbound
Local     IPv4    : 192.168.100.200
Global    IPv4    : 200.100.1.200
Reversible    : Y
Type          : Outbound
Total Ipv4 entries found: 2
```

表 11-6 コマンド出力

フィールド	説明
Global IPv4	パブリックIPv4アドレス。
Local IPv4	プライベートIPv4アドレス。
Reversible	逆アドレス変換が許可されているかどうか。 • Y:逆アドレス変換が許可されます。 • N:逆アドレス変換は許可されません。
Type	NO-PATエントリのタイプ: • インバウンド:インバウンドダイナミックNAT中に作成されたNO-PATエントリ。 • Outbound :送信ダイナミックNAT中に作成されたNO-PATエントリ。
Total Ipv4 entries found	IPv 4 NO-PATエントリの総数。

関連コマンド

- **nat inbound**
- **nat outbound**

11.1.9 display nat outbound

Syntax

display nat outbound

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat outbound コマンドは送信ダイナミック NAT 設定に関する情報を表示します。

例

送信ダイナミック NAT の設定を表示します。

<AP> display nat outbound

```
NAT outbound information:
```

```
Totally 2 NAT outbound rules.
Interface: Vlan-interface10
  Address group ID: 1
  Port-preserved: Y       NO-PAT: N  Reversible: N
  Rule name: acdefg
  Priority: 1000
  NAT counting: 0
  Config status: Active

Interface: Vlan-interface10
  ACL: 2037
  Address group ID: ---
  Port-preserved: N       NO-PAT: Y  Reversible: Y
  Rule name: abefg
  Priority: 1000
  NAT counting: 0
  Config status: Inactive
  Reasons for inactive status:
    The following items don't exist or aren't effective: ACL

Interface: Vlan-interface10
  ACL: 2100
  Address group ID: 2
  Port-preserved: N        NO-PAT: N  Reversible: N
  Priority: 0
  NAT counting: 0
  Config status: Active
```

表 11-7 コマンド出力

フィールド	説明
NAT outbound information	送信ダイナミックNAT設定に関する情報。
Totally n NAT outbound rules	送信ダイナミックNATルールの合計数。
Interface	送信ダイナミックNATルールが設定されているインタフェース。
ACL	IPv 4 ACLの番号または名前。送信ダイナミックNATルールにIPv 4 ACLが指定されていない場合、このフィールドにはハイフン (---) が表示されます。
Address group ID	送信ダイナミックNATルールで使用されるアドレスグループのID。アドレスグループが指定されていない場合、フィールドにはハイフン (---) が表示されます。

フィールド	説明
Address group name	NATアドレスグループの名前。アドレスグループ名が設定されていない場合、このフィールドは表示されません。
Port-preserved	PATのポート番号を保持しようとするかどうか。 ● Y:ポート番号を保持しようとします。 ● N:ポート番号の変換を許可します。
NO-PAT	NO-PATが使用されているかどうか。 ● Y:NO-PATが使用されます。 ● N:PATが使用されます。
Reversible	逆アドレス変換が許可されているかどうか。 ● Y:逆アドレス変換が許可されます。 ● N:逆アドレス変換は許可されません。
Rule name	NATルールの名前。
Priority	NATルールのプライオリティ。
Description	NATルールの説明です。ルールの説明が設定されていない場合、このフィールドは表示されません。
Configuration mode	装置の設定方法です。 ● 装置がNETCONFアクション操作を使用して設定されている場合、このフィールドにはNETCONF (action) が表示されます。 ● 装置が他を使用して設定されている場合、このフィールドは表示されません。

関連コマンド

nat outbound

11.1.10 display nat session

Syntax

display nat session [[**responder**] { **source-ip** *source-ip* | **destination-ip** *destination-ip* } *] [**brief** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

responder: NAT セッションをレスポンダ別に表示します。このキーワードを指定しない場合、このコマンドは NAT セッションを発信側別に表示します。

source-ip *source-ip*: source-ip 引数で指定された送信元 IP アドレスの NAT セッションを表示します。IP アドレスは、セッションの確立をトリガーするパケットの送信元 IP アドレスである必要があります。

destination-ip *destination-ip*: destination-ip 引数で指定された宛先 IP アドレスの NAT セッションを表示します。IP アドレスは、セッションの確立をトリガーするパケットの宛先 IP アドレスである必要があります。

brief: NAT セッションに関する簡単な情報を表示します。

verbose: NAT セッションに関する詳細情報を表示します。このキーワードを指定しない場合、このコマンドは NAT セッションに関する簡単な情報を表示します。

説明

display nat session コマンドは NAT セッションを表示します。

パラメータを指定しない場合、このコマンドはすべての NAT セッションを表示します。

例

NAT セッションに関する詳細情報を表示します。

<AP> display nat session verbose

```
Slot 0:
Initiator:
  Source     IP/port: 192.168.1.18/1877
  Destination IP/port: 192.168.1.55/22
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface10
  Source security zone: SrcZone
Responder:
  Source     IP/port: 192.168.1.55/22
  Destination IP/port: 192.168.1.10/1877
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: TCP(6)
  Inbound interface: Vlan-interface20
  Source security zone: DestZone
State: TCP_SYN_SENT
Application: SSH
Rule ID: -/-/-
Rule name:
```

```
Start time: 2011-07-29 19:12:36  TTL: 28s
Initiator->Responder:        1 packets        48 bytes
Responder->Initiator:        0 packets         0 bytes

Total sessions found: 1
```

表 11-8 コマンド出力

フィールド	説明
Initiator	イニシエータに関するセッション情報。
Responder	応答側に関するセッション情報。
Source IP/port	送信元IPアドレスおよびポート番号。
Destination IP/port	宛先IPアドレスおよびポート番号。
Global IP/port	パブリックIPアドレスおよびポート番号。
DS-Lite tunnel peer	DS-Liteトンネルインタフェースの宛先アドレス。セッションがどのDS-Liteトンネルにも属していない場合、このフィールドにはハイフン (-) が表示されます。
VPN instance/VLAN ID/Inline ID	次の情報を識別します。 • **VPN instance**–セッションが属するMPLS L 3 VPNインスタンス。VPNインスタンスフィールドは、現在のソフトウェアバージョンではサポートされていません。 • **VLAN ID**—レイヤ2転送のためにセッションが属するVLAN ID • **Inline ID**—レイヤ2転送のためにセッションが属するINLINE。 VPN instance、VLAN ID、またはInline IDが指定されていない場合、関連フィールドにはハイフン(-)が表示されます。
Protocol	トランスポート層プロトコルタイプ: DCCP、ICMP、Raw IP、SCTP、TCP、UDP、またはUDP-Lite。
Inbound interface	入力インタフェースです。
State	NATセッションのステータスです。
Application	FTPやDNSなどのアプリケーション層プロトコルタイプ。このフィールドには、既知でないポートによって識別されるプロトコルタイプのOTHERが表示されます。
Rule ID	セキュリティ・ポリシー・ルールのID。
Rule name	セキュリティ・ポリシー・ルールの名前。

フィールド	説明
Start time	セッションの開始時刻。
TTL	残りのNATセッションライフタイム (秒) 。
Initiator->Responder	送信側から応答側へのパケット数およびパケットバイト数。
Responder->Initiator	応答側から送信側へのパケット数およびパケットバイト数。
Total sessions found	セッションの合計数。

関連コマンド

reset nat session

11.1.11 display nat static

Syntax

display nat static

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nat static コマンドはスタティック NAT マッピングを表示します。

例

スタティック NAT マッピングを表示します。

<AP> display nat static

```
Static NAT mappings:
  Totally 2 inbound static NAT mappings.
  Net-to-net:
    Global IP    : 1.1.1.1 - 1.1.1.255
    Local IP     : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL          : 2000
```

```
    Reversible   : Y
    NAT counting : 0
    Rule name    : abcdefg
    Priority     : 1000
    Config status: Active

  IP-to-IP:
    Global IP    : 5.5.5.5
    Local IP     : 4.4.4.4
    ACL         : 2000
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
    NAT counting : 0
   Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: local VPN, global VPN,
and ACL.

Totally 2 outbound static NAT mappings.
  Net-to-net:
    Local IP     : 1.1.1.1 - 1.1.1.255
    Global IP    : 2.2.2.0
    Netmask      : 255.255.255.0
    ACL         : 2000
    Reversible   : Y
    Rule name    : abefg
    Priority     : 1000
    NAT counting : 0
    Config status: Active

  IP-to-IP:
    Local IP     : 4.4.4.4
    Global IP    : 5.5.5.5
    ACL:        : 2001
    Reversible   : Y
    Rule name    : abcd
    Priority     : 1000
    NAT counting : 0
    Config status: Inactive
    Reasons for inactive status:
      The following items don't exist or aren't effective: ACL.
```

```
Interfaces enabled with static NAT:
  Totally 2 interfaces enabled with static NAT.
  Interface: Vlan-interface20
    Config status: Active
```

表 11-9 コマンド出力

フィールド	説明
Static NAT mappings	スタティックNATマッピングの設定に関する情報。
Totally n inbound static NAT mappings	インバウンドスタティックNATマッピングの合計数。
Totally n outbound static NAT mappings	送信スタティックNATマッピングの合計数。
Net-to-net	Net-to-netスタティックNATマッピング。
IP-to-IP	1対1のスタティックNATマッピング。
Local IP	プライベートIPアドレスまたはアドレス範囲。
Global IP	パブリックIPアドレスまたはアドレス範囲。
Netmask	ネットワークマスク。
ACL	ACL番号または名前。ACLが指定されていない場合、このフィールドは表示されません。
Reversible	逆アドレス変換を許可するかどうか。逆アドレス変換が許可されている場合、このフィールドにはYと表示されます。逆アドレス変換が許可されていない場合、このフィールドは表示されません。
Interfaces enabled with static NAT	スタティックNATが有効になっているインタフェース。
Totally n interfaces enabled with static NAT	スタティックNATが有効になっているインタフェースの総数。
Interface	スタティックNATが有効になっているインタフェース。
Rule name	NATルールの名前。
Priority	NATルールのプライオリティ。
NAT counting	NATルールが一致した回数。
Description	NATルールの説明です。ルールの説明が設定されていない場合、このフィールドは表示されません。

フィールド	説明
Config status	スタティックNATマッピングのステータス（Activeまたは Inactive）。
Reasons for inactive status	スタティックNATマッピングが有効にならない理由。このフィールドは、Configステータスが Inactiveの場合に使用できます。

関連コマンド

- **nat static enable**
- **nat static inbound**
- **nat static inbound net-to-net**
- **nat static outbound**
- **nat static outbound net-to-net**

11.1.12 display nat statistics

Syntax

display nat statistics [**summary**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

summary: NAT 統計情報の要約を表示します。このキーワードを指定しない場合、このコマンドは詳細な NAT 統計情報を表示します。

説明

display nat statistics コマンドは NAT 統計情報を表示します。

例

NAT 統計情報の詳細情報を表示します。

<AP> display nat statistics

```
Slot 0:
  Session creation rate: 0
  Total session entries: 100
  Total EIM entries: 1
  Total inbound NO-PAT entries: 0
  Total outbound NO-PAT entries: 0
  Total static port block entries: 10
  Total dynamic port block entries: 15
  Active static port block entries: 0
  Active dynamic port block entries: 0
```

表 11-10 コマンド出力

フィールド	説明
Total session entries	NATセッションエントリの数。
Total EIM entries	EIMエントリの合計数。
Total inbound NO-PAT entries	インバウンドNO-PATエントリの合計数。

フィールド	説明
Total outbound NO-PAT entries	送信NO-PATエントリの合計数。
Total static port block entries	スタティック NAT 444マッピングの総数。
Total dynamic port block entries	作成できるダイナミックポートブロックマッピングの総数。これは、割り当てられたポートブロックと割り当てられていないポートブロックを含む、ダイナミック割り当てのポートブロックの数と同じです。
Active static port block entries	使用中のスタティックポートブロックマッピングの数。
Active dynamic port block entries	作成されたダイナミックポートブロックマッピングの数。これは、動的に割り当てられたポートブロックの数と同じです。

NAT 統計情報のサマリーを表示します。

<AP> display nat statistics summary

```
EIM: Total EIM entries.
SPB: Total static port block entries.
DPB: Total dynamic port block entries.
ASPB: Active static port block entries.
ADPB: Active dynamic port block entries.
Slot Sessions  EIM      SPB      DPB      ASPB     ADPB
0    100      1        10       15       0        0
```

表 11-11 コマンド出力

フィールド	説明
Sessions	NATセッションエントリの数。
EIM	EIMエントリの数。
SPB	スタティック NAT 444マッピングの数。
DPB	作成できるダイナミックポートブロックマッピングの数。これは、割り当てられたポートブロックと割り当てられていないポートブロックを含む、ダイナミック割り当てのポートブロックの数と同じです。
ASPB	使用中のスタティックポートブロックマッピングの数。
ADPB	作成されたダイナミックポートブロックマッピングの数。これは、動的に割り当てられたポートブロックの数と同じです。

11.1.13 nat address-group

Syntax

nat address-group *group-id* [**name** *group-name*]

undo nat address-group *group-id*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-id : NAT アドレスグループの ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: NAT アドレスグループに名前を割り当てます。*group-name* 引数は、1~63 文字のストリングで、大文字と小文字が区別されます。

説明

nat address-group コマンドは NAT アドレスグループを作成し、そのビューを移行するか、または既存の NAT アドレスグループのビューを移行します。

undo nat address-group コマンドは NAT アドレスグループを削除します。

NAT アドレスグループは、アドレス範囲のセットです。address コマンドを使用して、NAT アドレスグループにアドレス範囲を追加します。ダイナミック NAT は、パケットの送信元 IP アドレスをアドレスグループ内の IP アドレスに変換します。

例

#番号が 1 で名前が abc の NAT アドレスグループを作成します。

<AP> system-view

[AP] nat address-group 1 name abc

関連コマンド

- **address**
- **display nat address-group**
- **display nat all**
- **nat inbound**
- **nat outbound**

11.1.14 nat alg

Syntax

nat alg { all | dns | ftp | h323 | icmp-error | ils | mgcp | nbt | pptp | rsh | rtsp | sccp | sctp | sip | sqlnet | tftp | xdmcp }

undo nat alg { all | dns | ftp | h323 | icmp-error | ils | mgcp | nbt | pptp | rsh | rtsp | sccp | sctp | sip | sqlnet | tftp | xdmcp }

デフォルト

dns, ftp, icmp-error, rtsp, pptp：有効

その他：無効

View

System view

定義済みユーザロール

network-admin

パラメータ

all: サポートされているすべてのプロトコルに対して NAT ALG を有効にします。

dns: DNS の NAT ALG を有効にします。

ftp: FTP の NAT ALG を有効にします。

h323: H.323 の NAT ALG を有効にします。

icmp-error: ICMP エラーパケットの NAT ALG を有効にします。

ils: ILS の NAT ALG を有効にします。

mgcp: MGCP の NAT ALG を有効にします。

nbt: NBT の NAT ALG を有効にします。

pptp: PPTP の NAT ALG を有効にします。

rsh: RSH の NAT ALG を有効にします。

rtsp: RTSP の NAT ALG を有効にします。

sccp: SCCP の NAT ALG を有効にします。

sctp: SCTP の NAT ALG を有効にします。

sip: SIP の NAT ALG を有効にします。

sqlnet: SQLNET 用の NAT ALG を有効にします。

tftp: TFTP の NAT ALG を有効にします。

xdmcp: XDMCP の NAT ALG を有効にします。

説明

nat alg コマンドは、指定されたプロトコルまたはサポートされているすべてのプロトコルに対して NAT ALG を有効にします。

undo nat alg コマンドは、指定したプロトコルまたはサポートされているすべてのプロトコルの NAT ALG を無効にします。

NAT ALG は､アプリケーション層ペイロード内のアドレスまたはポート情報を変換して、接続の確立を保証します。

たとえば、FTP アプリケーションには、データ接続と制御接続が含まれます。データ接続の IP アドレスとポート番号は、制御接続のペイロード情報によって異なります。これには、NAT ALG がアドレスおよびポート情報を変換してデータ接続を確立する必要があります。

例

#FTP の NAT ALG を有効にします。

<AP> system-view

[AP] nat alg ftp

関連コマンド

display udp statistics

11.1.15 nat icmp-error reply

Syntax

nat icmp-error reply

undo nat icmp-error reply

デフォルト

NAT 障害時の ICMP エラーメッセージの送信無効

View

System view

定義済みユーザロール

network-admin

説明

nat icmp-error reply コマンドは NAT 障害時の ICMP エラーメッセージの送信を有効にします。

undo nat icmp-error reply コマンドはデフォルト状態に戻します。

NAT 障害時の ICMP エラーメッセージの送信を無効にすると、不要なパケットが減少し、帯域幅が節約され、デバイスの IP アドレスがパブリックネットワークに公開されなくなります。

このコマンドは traceroute に必要です。

例

#NAT 失敗時の ICMP エラーメッセージの送信を有効にします。

<AP> system-view

[AP] nat icmp-error reply

11.1.16 nat inbound

Syntax

nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** { *group-id* | **name** *group-name* } [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]

undo nat inbound { *ipv4-acl-number* | **name** *ipv4-acl-name* }

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、すべてを指定することはできません。

address-group: アドレス変換のアドレスグループを指定します。

group-id: アドレスグループ ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: アドレスグループ名を指定します。1~63 文字で、大文字と小文字は区別されません。

no-pat: NO-PAT モードを使用します。このキーワードを指定しない場合は、PAT が使用されます。PAT では、TCP、UDP、および ICMP クエリーパケットだけがサポートされます。ICMP パケットの場合、送信元ポート番号として ICMP ID が使用されます。

reversible: 逆アドレス変換をイネーブルにします。逆アドレス変換は、既存の NO-PAT エントリを使用して、内部ネットワークからアクティブに開始された接続の宛先アドレスを外部ネットワークに変換します。

add-route: 変換後に自動的に送信元アドレスにルートを追加します。出力インタフェースは NAT インタフェースで、ネクストホップは変換前の送信元アドレスです。

rule *rule-name*: ルールの名前を指定します。大文字と小文字が区別され、1~63 文字のストリングで指定します。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、クオーテーションマーク(") 、またはアット記号 (@) です。このオプションを指定しない場合、規則に名前はありません。

priority *priority*: ルールのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、同じタイプの NAT 規則の中で優先順位が最も低くなります。

disable: 受信ダイナミック NAT ルールを無効にします。このキーワードを指定しない場合、ルールは有効になります。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

description *text*: 受信ダイナミック NAT ルールの説明を指定します。text 引数は、大文字と小文字を区別しない 1~63 文字の文字列です。

説明

nat inbound コマンドは受信ダイナミック NAT ルールを設定します。

undo nat inbound コマンドは受信ダイナミック NAT ルールを削除します。

受信ダイナミック NAT は、ACL によって許可された受信パケットの送信元 IP アドレスをアドレスグループ内の IP アドレスに変換します。

受信ダイナミック NAT は、次のモードをサポートします。

- [PAT] :IP アドレス変換とポート変換の両方を実行します。
- [NO-PAT] :IP アドレス変換だけを実行します。

NO-PAT モードでは、逆アドレス変換がサポートされます。逆アドレス変換では、ACL 逆マッチングを使用して、変換するパケットを識別します。ACL リバースマッチングは次のように機能します。

- パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
- 一致する NO-PAT エントリに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

受信ダイナミック NAT は通常、次のいずれかと連携して双方向 NAT を実装します。

- 送信ダイナミック NAT (nat outbound コマンド) 。
- 送信スタティック NAT (nat static コマンド) 。

アドレスグループは、nat inbound コマンドと nat outbound コマンドの両方で使用できません。nat inbound コマンドでは、PAT モードと NO-PAT モードの両方で使用できません。

内部ネットワークと外部ネットワークが存在するサブネットが重複している場合は、add-route キーワードを指定しないでください。その他のネットワークシナリオの場合:

- add-route キーワードを指定すると、デバイスはパケットの変換後に自動的に送信元アドレスにルートを追加します。宛先アドレスは NAT アドレスグループ内の NAT アドレス、出力インタフェースはコマンドが実行されるインタフェース、ネクストホップは変換前の送信元アドレスです。
- add-route キーワードを指定しない場合は、ルートを手動で追加する必要があります。自動ルート追加は低速であるため、手動でルートを追加することをお勧めします。

ACL は、インタフェース上の 1 つの受信ダイナミック NAT ルールだけで使用できます。

1 つのインタフェースに複数の受信ダイナミック NAT ルールを設定できます。

同じプライオリティ値で設定された受信ダイナミック NAT ルールは、その ACL を使用して照合されます。

- 名前付き ACL を持つ NAT ルールは、名前なし ACL を持つ NAT ルールよりも優先順位が高くなります。
- 名前付き ACL を持つ NAT ルールは、ACL 名のアルファベット順に照合されます。
- 名前なし ACL を持つ NAT ルールは、ACL 番号の降順で照合されます。

例

#サブネット 10.110.10.0/24 からのパケットだけを通過させるには、ACL 2001 を設定します。

<AP> system-view

[AP] acl basic 2001

[AP-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255

[AP-acl-ipv4-basic-2001] rule deny

[AP-acl-ipv4-basic-2001] quit

#アドレスグループ 1 を作成し、アドレス範囲 202.110.10.10~202.110.10.12 をグループに追加します。

[AP] nat address-group 1

[AP-address-group-1] address 202.110.10.10 202.110.10.12

[AP-address-group-1] quit

#インバウンド NO-PAT ルールをインタフェース VLAN インタフェース 10 に設定します。NAT は、受信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換し、変換されたパケットのルートを自動的に追加します。ルール名を abc に、優先順位を 0 に設定します。

[AP] interface vlan-interface 10

[AP-Vlan-interface10] nat inbound 2001 address-group 1 no-pat add-route rule abc priority 0

関連コマンド

- **display nat all**
- **display nat inbound**
- **display nat no-pat**

11.1.17 nat inbound rule move

Syntax

nat inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

View

Interface view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1: 移動するルールの名前を指定します。

after: ルール nat-rule-name 1 をルール nat-rule-name 2 の後の行 (参照ルールと呼ばれます) に移動します。参照規則の優先度の値は変更されません。移動されたルールの優先度の値は、参照ルールの優先度の値に 1 を加えた値と等しくなります。

before: ルール nat-rule-name 1 をルール nat-rule-name 2 の前の行に移動します。参照規則の優先度の値は変更されません。移動したルールの優先度値は、参照ルールの優先度値から 1 を引いた値と等しくなります。

nat-rule-name2: 移動する NAT 規則の参照規則として、NAT 規則の名前を指定します。

説明

nat inbound rule move コマンドは受信ダイナミック NAT ルールのプライオリティを変更します。

このコマンドは、名前付きインバウンドダイナミック NAT ルールにのみ適用できます。

ルールリストの前の方に表示されている NAT ルールは、パケットマッチングの優先順位が高くなります。

例

#インバウンドダイナミック NAT ルール abc を、ルール def の前の行に移動します。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] nat inbound rule move abc before def

関連コマンド

nat inbound

11.1.18 nat log alarm

Syntax

nat log alarm

undo nat log alarm

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nat log alarm コマンドは NAT アラームのログを有効にします。

undo nat log alarm コマンドは NAT アラームのログを無効にします。

NAT リソースが十分でない場合、変換が必要なパケットはドロップされます。NO-PAT では、NAT リソースはパブリック IP アドレスを参照します。EIM PAT では、NAT リソースはパブリック IP アドレスおよびポートを参照します。NAT 444 では、NAT リソースはパブリック IP アドレス、ポートブロック、またはポートブロック内のポートを参照します。NAT アラームログは NAT リソースの使用状況を監視し、NAT リソースが十分でない場合はログを出力します。

NAT のアラームログを設定する前に、カスタム NAT ログ生成および出力機能を設定する必要があります。

このコマンドは、nat log enable コマンドを使用して NAT ログを有効にした後にだけ有効になります。

例

#NAT アラームログを有効にします。

<AP> system-view

[AP] nat log alarm

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

11.1.19 nat log enable

Syntax

nat log enable [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat log enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

acl: ACL を指定します。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

説明

nat log enable コマンドは NAT のログを有効にします。

undo nat log enable コマンドは NAT のログを無効にします。

NAT セッションログ、または NAT アラームログを有効にする前に、NAT ログを有効にする必要があります。

acl キーワードは、NAT セッションログに対してだけ有効です。ACL が指定されている場合、許可ルールに一致するフローが NAT セッションログをトリガーすることがあります。ACL を指定しない場合、NAT によって処理されるすべてのフローが NAT セッションログをトリガーする可能性があります。

例

#NAT ログを有効にします。

<AP> system-view

[AP] nat log enable

関連コマンド

- **display nat all**
- **display nat log**

- **nat log alarm**
- **nat log flow-active**
- **nat log flow-begin**
- **nat log flow-end**

11.1.20 nat log flow-active

Syntax

nat log flow-active *time-value*

undo nat log flow-active

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: アクティブ NAT フローのログ間隔を 10~120 分の範囲で指定します。

説明

nat log flow-active コマンドは、アクティブな NAT フローのログを有効にし、ログ間隔を設定します。

undo nat log flow-active コマンドはアクティブな NAT フローのログを無効にします。

アクティブ NAT フローは、長時間続く NAT セッションです。ログ機能は、アクティブな NAT フローを定期的にログすることで、アクティブな NAT フローを追跡するのに役立ちます。

アクティブ NAT フローのログが有効になるのは、NAT ログを有効にした場合だけです。

例

#アクティブな NAT フローのログを有効にし、ログ間隔を 10 分に設定します。

<AP> system-view

[AP] nat log flow-active 10

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

11.1.21 nat log flow-begin

Syntax

nat log flow-begin

undo nat log flow-begin

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nat log flow-begin コマンドは NAT セッション確立イベントのログを有効にします。

undo nat log flow-begin コマンドは NAT セッション確立イベントのログを無効にします。

NAT セッション確立イベントのログは、NAT ログを有効にした後にだけ有効になります。

例

#NAT セッション確立イベントのログを有効にします。

<AP> system-view

[AP] nat log flow-begin

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

11.1.22 nat log flow-end

Syntax

nat log flow-end

undo nat log flow-end

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nat log flow-end コマンドは NAT セッション削除イベントのログを有効にします。

undo nat log flow-end コマンドは NAT セッション削除イベントのログを無効にします。

NAT セッション削除イベントのログは、NAT ログを有効にした後にだけ有効になります。

例

#NAT セッション削除イベントのログを有効にします。

<AP> system-view

[AP] nat log flow-end

関連コマンド

- **display nat all**
- **display nat log**
- **nat log enable**

11.1.23 nat mapping-behavior endpoint-independent

Syntax

nat mapping-behavior endpoint-independent [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }]

undo nat mapping-behavior endpoint-independent

デフォルト

Address and Port-Dependent Mapping

View

System view

定義済みユーザロール

network-admin

パラメータ

acl: Endpoint-Independent Mapping の適用可能なスコープを定義する ACL を指定します。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

説明

nat mapping-behavior endpoint-independent コマンドは PAT に対して EMI（Endpoint-Independent Mapping）モードを指定します。

undo nat mapping-behavior endpoint-independent コマンドはデフォルトに戻します。

PAT では、次の NAT マッピングモードがサポートされています。

- Endpoint-Independent Mapping:同じ送信元およびポートから任意の宛先へのパケットに、同じ IP およびポートマッピング（EIM エントリ）を使用します。EIM では、変換された IP アドレスとポートを使用して、外部ホストから内部ホストにアクセスできます。異なる NAT ゲートウェイの背後にある内部ホストが相互にアクセスできるようにします。
- Address and Port-Dependent Mapping :同じ送信元 IP およびポートを持つパケットに対して、異なる宛先 IP アドレスおよびポートへの異なる IP およびポートマッピングを使用します。APDM では、内部ホストがすでに外部ホストにアクセスしている場合にのみ、外部ホストが内部ホストにアクセスできます。これは安全ですが、異なるNAT ゲートウェイの背後にある内部ホストが相互にアクセスすることはできません。

このコマンドは、送信 PAT だけで有効になります。Address and Port-Dependent Mapping は、受信 PAT に常に適用されます。

ACL を指定すると、Endpoint-Independent Mapping が ACL によって許可されたパケットに適用されます。ACL を指定しない場合、Endpoint-Independent Mapping はすべてのパケットに適用されます。

例

#アドレス変換用のすべてのパケットに、エンドポイントに依存しないマッピングモードを適用します。

<AP> system-view

[AP] nat mapping-behavior endpoint-independent

#FTP および HTTP パケットにはエンドポイントに依存しないマッピングモードを適用し、アドレス変換のために他のパケットにはアドレスおよびポート依存マッピングモードを適用します。

<AP> system-view

[AP] acl advanced 3000

[AP-acl-ipv4-adv-3000] rule permit tcp destination-port eq 80

[AP-acl-ipv4-adv-3000] rule permit tcp destination-port eq 21

[AP-acl-ipv4-adv-3000] quit

[AP] nat mapping-behavior endpoint-independent acl 3000

関連コマンド

nat outbound

display nat eim

11.1.24 nat outbound

Syntax

NO-PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] **address-group** { *group-id* | **name** *group-name* } **no-pat** [**reversible**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** *text*]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

PAT:

nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*] [**address-group** { *group-id* | **name** *group-name* }] [**port-preserved**] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** text]

undo nat outbound [*ipv4-acl-number* | **name** *ipv4-acl-name*]

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

ipv4-acl-number: ipv 4-acl-number:2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

address-group: NAT のアドレスグループを指定します。アドレスグループを指定しない場合、インタフェースの IP アドレスが NAT アドレスとして使用されます。Easy IP が使用されている。

group-id: アドレスグループ ID を指定します。この引数の値の範囲は 0 から 65535 です。

name *group-name*: アドレスグループ名を指定します。1~63 文字で、大文字と小文字は区別されません。

no-pat: NO-PAT モードを使用します。このキーワードを指定しない場合は、PAT が使用されます。PAT では、TCP、UDP、および ICMP クエリーパケットだけがサポートされます。ICMP パケットの場合、送信元ポート番号として ICMP ID が使用されます。

reversible: 逆アドレス変換を有効にします。逆アドレス変換では、既存の NO-PAT エントリを使用して、外部ネットワークからアクティブに開始された接続の宛先アドレスを内部ネットワークに変換します。

port-preserved: PAT のポート番号を保持しようとします。

rule *rule-name*: ルールの名前を指定します。大文字と小文字が区別され、1~63 文字のストリングで指定します。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、クオーテーションマーク (") 、またはアット記号 (@) です。このオプションを指定しない場合、規則に名前はありません。

priority *priority*: ルールのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、同じタイプの NAT 規則の中で優先順位が最も低くなります。

disable: 送信ダイナミック NAT ルールを無効にします。このキーワードを指定しない場合、ルールは有効になります。

description *text*: 送信ダイナミック NAT ルールの説明を指定します。text 引数は、大文字と小文字を区別しない 1~63 文字の文字列です。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat outbound コマンドは送信ダイナミック NAT 規則を設定します。

undo nat outbound コマンドは送信ダイナミック NAT 規則を削除します。

送信ダイナミック NAT は通常、外部ネットワークに接続されたインタフェースで設定されます。1 つのインタフェースに複数の送信ダイナミック NAT ルールを設定できます。

送信ダイナミック NAT は、次のモードをサポートします。

- PAT :IP アドレス変換とポート変換の両方を実行します。PAT モードでは、エンドポイントに依存しないマッピング動作が使用されている場合、外部ホストは内部ホストにアクティブにアクセスできます。
- NO-PAT :IP アドレス変換だけを実行します。reversible キーワードを指定した場合、NO-PAT モードでは、外部ホストが内部ホストにアクティブにアクセスできます。ACL が指定されている場合、リバースアドレス変換は ACL リバースマッチングで許可されたパケットだけに適用されます。ACL リバースマッチングは次のように機能します。
  - □ パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - □ 一致する NO-PAT エントリに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

NAT アドレスグループを指定する場合は、次の制約事項および注意事項に従ってください。

- アドレスグループは、nat inbound コマンドと nat outbound コマンドの両方で使用できません。
- nat outbound コマンドでは、PAT モードと NO-PAT モードの両方でアドレスグループを使用できません。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL は、インタフェース上の 1 つの送信ダイナミック NAT ルールだけで使用できます。
- ACL を指定すると、NAT は ACL によって許可された送信パケットの送信元 IP アドレスをアドレスグループの IP アドレスに変換します。ACL を指定しない場合、NAT はすべてのパケットを変換します。
- インタフェースに ACL が設定されている送信ダイナミック NAT ルールは、ACL が設定されていないルールよりも優先されます。ACL ベースのダイナミック NAT ルールが 2 つ設定されている場合、ACL 番号が大きい方のルールのプライオリティが高くなります。

同じプライオリティ値で設定された送信ダイナミック NAT ルールと ACL は、ルール内の ACL を使用して照合されます。

- 名前付き ACL を持つ NAT ルールは、名前なし ACL を持つ NAT ルールよりも優先順位が高くなります。
- 名前付き ACL を持つ NAT ルールは、ACL 名のアルファベット順に照合されます。
- 名前なし ACL を持つ NAT ルールは、ACL 番号の降順で照合されます。

例

#サブネット 10.110.10.0/24 からのパケットだけを通過させるには、ACL 2001 を設定します。

<AP> system-view

[AP] acl basic 2001

[AP-acl-ipv4-basic-2001] rule permit source 10.110.10.0 0.0.0.255

[AP-acl-ipv4-basic-2001] rule deny

[AP-acl-ipv4-basic-2001] quit

#アドレスグループ 1 を作成し、アドレス範囲 202.110.10.10~202.110.10.12 をグループに追加します。

[AP] nat address-group 1

[AP-address-group-1] address 202.110.10.10 202.110.10.12

[AP-address-group-1] quit

#インタフェース VLAN インタフェース 10 の送信ダイナミック PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。

[AP] interface vlan-interface 10

[AP-Vlan-interface10] nat outbound 2001 address-group 1

[AP-Vlan-interface10] quit

#インタフェース VLAN インタフェース 10 で送信 NO-PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。

[AP] interface vlan-interface 10

[AP-Vlan-interface10] nat outbound 2001 address-group 1 no-pat

[AP-Vlan-interface10] quit

#VLAN インタフェース 10 の IP アドレスを変換後のアドレスとして使用するには、Easy IP を有効にします。

[AP] interface Vlan-interface 10

[AP-Vlan-interface10] nat outbound 2001

[AP-Vlan-interface10] quit

#VLAN インタフェース 10 で送信 NO-PAT ルールを設定して、ACL 2001 で許可された送信パケットの送信元アドレスをアドレスグループ 1 のアドレスに変換します。逆アドレス変換を有効にします。

[AP] interface Vlan-interface 10

[AP-Vlan-interface10] nat outbound 2001 address-group 1 no-pat reversible

関連コマンド

- **display nat eim**
- **display nat outbound**
- **nat mapping-behavior**

11.1.25 nat outbound rule move

Syntax

nat outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

View

Interface view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1: 移動する NAT ルールの名前を指定します。

after: ルール nat-rule-name 1 をルール nat-rule-name 2 の後の行 (参照ルールと呼ばれます) に移動します。参照規則の優先度の値は変更されません。移動されたルールの優先度の値は、参照ルールの優先度の値に 1 を加えた値と等しくなります。

before: ルール nat-rule-name 1 をルール nat-rule-name 2 の前の行に移動します。参照規則の優先度の値は変更されません。移動したルールの優先度値は、参照ルールの優先度値から 1 を引いた値と等しくなります。

nat-rule-name2: 移動する NAT 規則の参照規則として、NAT 規則の名前を指定します。

説明

nat outbound rule move コマンドは送信ダイナミック NAT ルールのプライオリティを変更します。

このコマンドは、名前付き送信ダイナミック NAT 規則にだけ適用できます。

ルールリストの前の方に表示されている NAT ルールは、パケットマッチングの優先順位が高くなります。

例

#送信ダイナミック NAT ルール abc を、ルール def の前の行に移動します。

<AP> system-view

[AP] interface vlan-interface 10

[AP-Vlan-interface10] nat outbound rule move abc before def

関連コマンド

nat outbound

11.1.26 nat static enable

Syntax

nat static enable

undo nat static enable

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

nat static enable コマンドはインタフェースでスタティック NAT を有効にします。

undo nat static enable コマンドはインタフェースでスタティック NAT を無効にします。

スタティック NAT マッピングがインタフェースで有効になるのは、そのインタフェースでスタティック NAT が有効になってからです。

例

#プライベート IP アドレス 192.168.1.1 とパブリック IP アドレス 2.2.2.2 の間の送信スタティック NAT マッピングを設定し、VLAN インタフェース 10 でスタティック NAT を有効にします。

<AP> system-view

[AP] nat static outbound 192.168.1.1 2.2.2.2

[AP] interface vlan-interface 10

[AP-Vlan-interface10] nat static enable

関連コマンド

- **display nat all**
- **display nat static**
- **nat static**
- **nat static net-to-net**

11.1.27 nat static inbound

Syntax

nat static inbound *global-ip local-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** text]

undo nat static inbound *global-ip local-ip*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

global-ip: パブリック IP アドレスを指定します。

local-ip: プライベート IP アドレスを指定します。

acl: 外部ネットワークにアクセスできる内部ホストを識別する ACL を指定します。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

reversible: 内部ネットワークからアクティブに開始された接続に対して、プライベート IP アドレスへの逆アドレス変換を有効にします。

rule *rule-name*: マッピングの名前を指定します。大文字と小文字が区別され、1~63 文字の文字列になります。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、クオーテーションマーク (") 、またはアット記号 (@) です。このオプションを指定しない場合、マッピングに名前はありません。

priority *priority*: マッピングのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、マッピングのプライオリティは同じタイプの NAT 規則の中で最も低くなります。

disable: 1 対 1 の受信スタティックマッピングを無効にします。このキーワードを指定しない場合、マッピングは有効になります。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

description *text*: 1 対 1 のインバウンドスタティックマッピングの説明を指定します。*text* の引数は、大文字と小文字を区別しない 1～63 文字の文字列です。

説明

nat static inbound コマンドは受信スタティック NAT の 1 対 1 マッピングを設定します。

undo nat static inbound コマンドは受信スタティック NAT の 1 対 1 マッピングを削除します。

外部ネットワークから内部ネットワークへのパケットの送信元 IP アドレスが global-ip と一致する場合、送信元 IP アドレスは local-ip に変換されます。内部ネットワークから外部ネットワークへのパケットの宛先 IP アドレスが local-ip と一致する場合、宛先 IP アドレスは global-ip に変換されます。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL を指定しない場合、すべての受信パケットの送信元アドレスとすべての送信パケットの宛先アドレスが変換されます。
- ACL を指定し、reversible キーワードを指定しない場合、ACL によって許可された受信パケットの送信元アドレスが変換されます。内部ネットワークからアクティブに開始された接続の宛先アドレスは、プライベート IP アドレスに変換されません。
- ACL と reversible キーワードの両方を指定すると、ACL によって許可された受信パケットの送信元アドレスが変換されます。内部ネットワークからプライベート IP アドレスへアクティブに開始された接続のパケットが ACL 逆マッチングによって許可される場合、宛先アドレスは変換されます。ACL リバースマッチングは次のように機能します。
  - □ パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - □ マッピングに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

スタティック NAT とダイナミック NAT の両方がインタフェースに設定されている場合、スタティック NAT はダイナミック NAT よりも優先されます。

nat static inbound コマンドと nat static inbound net-to-net コマンドを使用すると、複数のインバウンドスタティック NAT マッピングを設定できます。

同じプライオリティ値と ACL で設定されたインバウンドスタティック NAT の 1 対 1 マッピングは、マッピングの ACL を使用して照合されます。

- 名前付き ACL を持つマッピングは、名前なし ACL を持つマッピングよりも優先順位が高くなります。
- 名前付き ACL を持つマッピングは、ACL 名のアルファベット順に一致します。
- 名前なし ACL を持つマッピングは、ACL 番号の降順で照合されます。

例

#パブリック IP アドレス 2.2.2.2 とプライベート IP アドレス 192.168.1.1 の間のインバウンドスタティック NAT マッピングを設定します。

<AP> system-view

[AP] nat static inbound 2.2.2.2 192.168.1.1

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

11.1.28 nat static inbound net-to-net

Syntax

nat static inbound net-to-net *global-start-address global-end-address* **local** *local-network* { *mask-length* | *mask* } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static inbound net-to-net *global-start-address global-end-address* **local** *local-network* { *mask-length* | *mask* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

global-start-address global-end-address: 最大 255 個のアドレスを含むことができるパブリックアドレス範囲を指定します。global-end-address は global-start-address より小さくできません。同じ場合、パブリックアドレスは 1 つだけ指定されます。

local-network: プライベートネットワークアドレスを指定します。

mask-length: プライベートネットワークアドレスのマスク長を 8~31 の範囲で指定します。

mask: プライベートネットワークアドレスのマスクを指定します。

acl: 外部ネットワークにアクセスできる内部ホストを識別する ACL を指定します。

ipv4-acl-number: 2000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

reversible: 内部ネットワークからアクティブに開始された接続に対して、プライベート IP アドレスへの逆アドレス変換を有効にします。

rule *rule-name*: マッピングの名前を指定します。大文字と小文字が区別され、1~63 文字の文字列になります。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、クオーテーションマーク (") 、またはアット記号 (@) です。このオプションを指定しない場合、マッピングに名前はありません。

priority *priority*: マッピングのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、マッピングのプライオリティは同じタイプの NAT 規則の中で最も低くなります。

disable: net-to-net 受信スタティックマッピングを無効にします。このキーワードを指定しない場合、マッピングは有効になります。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat static inbound net-to-net コマンドは受信スタティック NAT の net to net マッピングを設定します。

undo nat static inbound net-to-net コマンドは受信スタティック NAT の net to net マッピングを削除します。

開始アドレスと終了アドレスでパブリックネットワークを指定し、プライベートアドレスとマスクでプライベートネットワークを指定します。

外部ネットワークからのパケットの送信元アドレスがパブリックアドレス範囲と一致する場合、送信元アドレスはプライベートアドレス範囲内のプライベートアドレスに変換されます。内部ネットワークからのパケットの宛先アドレスがプライベートアドレス範囲と一致する場合、宛先アドレスはパブリックアドレス範囲内のパブリックアドレスに変換されます。

パブリック終了アドレスは、パブリック開始アドレスとプライベートネットワークマスクによって決定されるサブネット内の最大 IP アドレスより大きくすることはできません。たとえば、プライベートアドレスが 2.2.2.0 でマスクが 255.255.255.0、パブリック開始アドレスが 1.1.1.100 の場合、パブリック終了アドレスはサブネット 1.1.1.0/24 内で最大の IP アドレスである 1.1.1.255 より大きくすることはできません。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL を指定しない場合、すべての受信パケットの送信元アドレスとすべての送信パケットの宛先アドレスが変換されます。
- ACL を指定し、reversible キーワードを指定しない場合、ACL によって許可された受信パケットの送信元アドレスが変換されます。内部ネットワークからアクティブに開始された接続の宛先アドレスは、プライベート IP アドレスに変換されません。
- ACL と reversible キーワードの両方を指定すると、ACL によって許可された受信パケットの送信元アドレスが変換されます。内部ネットワークからプライベート IP アドレスへアクティブに開始された接続のパケットが ACL 逆マッチングによって許可される場合、宛先アドレスは変換されます。ACL リバースマッチングは次のように機能します。
  - □ パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - □ マッピングに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

スタティック NAT とダイナミック NAT の両方がインタフェースに設定されている場合、スタティック NAT はダイナミック NAT よりも優先されます。

nat static inbound コマンドと nat static inbound net-to-net コマンドを使用すると、複数のインバウンドスタティック NAT マッピングを設定できます。

同じプライオリティ値と ACL で設定されたインバウンドスタティック NAT のネット/ネットマッピングは、マッピングで ACL を使用して照合されます。

- 名前付き ACL を持つマッピングは、名前なし ACL を持つマッピングよりも優先順位が高くなります。
- 名前付き ACL を持つマッピングは、ACL 名のアルファベット順に一致します。
- 名前なし ACL を持つマッピングは、ACL 番号の降順で照合されます。

例

#パブリックネットワークアドレス 202.100.1.0/24 とプライベートネットワークアドレス 192.168.1.0/24 の間のインバウンドスタティック NAT を設定します。

<AP> system-view

[AP] nat static inbound net-to-net 202.100.1.1 202.100.1.255 local 192.168.1.0 24

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

11.1.29 nat static inbound rule move

Syntax

nat static inbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

View

System view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1: 移動する NAT ルールの名前を指定します。

after: ルール nat-rule-name 1 をルール nat-rule-name 2 の後の行 (参照ルールと呼ばれます) に移動します。参照規則の優先度の値は変更されません。移動されたルールの優先度の値は、参照ルールの優先度の値に 1 を加えた値と等しくなります。

before: ルール nat-rule-name 1 をルール nat-rule-name 2 の前の行に移動します。参照規則の優先度の値は変更されません。移動したルールの優先度値は、参照ルールの優先度値から 1 を引いた値と等しくなります。

nat-rule-name2: 移動する NAT 規則の参照規則として、NAT 規則の名前を指定します。

説明

nat static inbound rule move コマンドは 1 対 1 の受信スタティック NAT ルールのプライオリティを変更します。

このコマンドは、名前付き受信 1 対 1 スタティック NAT ルールにのみ適用されます。

ルールリストの前の方に表示されている NAT ルールは、パケットマッチングの優先順位が高くなります。

例

#インバウンド 1 対 1 スタティック NAT ルール abc を、インバウンド 1 対 1 スタティック NAT ルール def の前の行に移動します。

<AP> system-view

[AP] nat static inbound rule move abc before def

関連コマンド

nat static inbound

11.1.30 nat static outbound

Syntax

nat static outbound *local-ip global-ip* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**] [**description** *text*]

undo nat static outbound *local-ip global-ip*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

local-ip: プライベート IP アドレスを指定します。

global-ip: パブリック IP アドレスを指定します。

acl: 内部ホストがアクセスできる宛先 IP アドレスを定義する ACL を指定します。

ipv4-acl-number: 3000~3999 の番号で ACL を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

reversible: 外部ネットワークからアクティブに開始された接続の逆アドレス変換を、パブリック IP アドレスに有効にします。

rule *rule-name*: マッピングの名前を指定します。大文字と小文字が区別され、1~63 文字の文字列になります。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、クオーテーションマーク (") 、またはアット記号 (@) です。このオプションを指定しない場合、マッピングに名前はありません。

priority *priority*: マッピングのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、マッピングのプライオリティは同じタイプの NAT 規則の中で最も低くなります。

disable: 1 対 1 の送信スタティックマッピングを無効にします。このキーワードを指定しない場合、マッピングは有効になります。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

description *text*: 1 対 1 アウトバウンドスタティックマッピングの説明を指定します。text 引数は、大文字と小文字を区別しない 1～63 文字の文字列です。

説明

nat static outbound コマンドは送信スタティック NAT の 1 対 1 マッピングを設定します。

undo nat static outbound コマンドは送信スタティック NAT の 1 対 1 マッピングを削除します。

送信パケットの送信元 IP アドレスが local-ip と一致する場合、IP アドレスは global-ip に変換されます。受信パケットの宛先 IP アドレスが global-ip と一致する場合、宛先 IP アドレスは local-ip に変換されます。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL を指定しない場合、すべての送信パケットの送信元アドレスとすべての受信パケットの宛先アドレスが変換されます。
- ACL を指定し、reversible キーワードを指定しない場合、ACL によって許可された送信パケットの送信元アドレスが変換されます。外部ネットワークからアクティブに開始された接続の宛先アドレスは、パブリック IP アドレスに変換されません。
- ACL と reversible キーワードの両方を指定すると、ACL によって許可された送信パケットの送信元アドレスが変換されます。外部ネットワークからパブリック IP アドレスに対してアクティブに開始された接続のパケットが ACL リバースマッチングによって許可される場合、宛先アドレスは変換されます。ACL リバースマッチングは次のように機能します。
  - □ パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - □ マッピングに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

スタティック NAT は、両方がインタフェースに設定されている場合、ダイナミック NAT よりも優先されます。

nat static outbound コマンドと nat static outbound net-to-net コマンドを使用すると、複数の送信スタティック NAT マッピングを設定できます。

同じプライオリティ値と ACL で設定された送信スタティック NAT の 1 対 1 マッピングは、マッピングの ACL を使用して照合されます。

- 名前付き ACL を持つマッピングは、名前なし ACL を持つマッピングよりも優先順位が高くなります。
- 名前付き ACL を持つマッピングは、ACL 名のアルファベット順に一致します。
- 名前なし ACL を持つマッピングは、ACL 番号の降順で照合されます。

例

#パブリック IP アドレス 2.2.2.2 とプライベート IP アドレス 192.168.1.1 の間の送信スタティック NAT マッピングを設定します。

<AP> system-view

[AP] nat static outbound 192.168.1.1 2.2.2.2

#外部へのスタティック NAT を設定し、内部ユーザ 192.168.1.1 がパブリック IP アドレス 2.2.2.2 を使用して外部ネットワーク 3.3.3.0/24 にアクセスできるようにします。

<AP> system-view

[AP] acl advanced 3001

[AP-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255

[AP-acl-ipv4-adv-3001] quit

[AP] nat static outbound 192.168.1.1 2.2.2.2 acl 3001

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

11.1.31 nat static outbound net-to-net

Syntax

nat static outbound net-to-net *local-start-address local-end-address* **global** *global-network* { *mask-length* | *mask* } [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* } [**reversible**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**counting**]

undo nat static outbound net-to-net *local-start-address local-end-address* **global** *global-network* { *mask-length* | *mask* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

local-start-address local-end-address: 最大 255 個のアドレスを含むことができるプライベートアドレス範囲を指定します。local-end-address は local-start-address より小さくできません。同じ場合は、プライベートアドレスを 1 つだけ指定します。

global-network: パブリックネットワークアドレスを指定します。

mask-length: パブリックネットワークアドレスのマスク長を 8~31 の範囲で指定します。

mask: パブリックネットワークアドレスのマスクを指定します。

acl: 内部ホストがアクセスできる宛先 IP アドレスを定義する ACL を指定します。

ipv4-acl-number: 2000~3999 の範囲で ACL 番号を指定します。

name *ipv4-acl-name*: ACL を名前で指定します。1~63 文字で、大文字と小文字は区別されません。ACL 名は英字で始まる必要があり、混乱を避けるために、all を指定することはできません。

reversible: 外部ネットワークからアクティブに開始された接続の逆アドレス変換を、パブリック IP アドレスに有効にします。

rule *rule-name*: マッピングの名前を指定します。大文字と小文字が区別され、1~63 文字の文字列になります。バックスラッシュ (¥) 、スラッシュ (/) 、コロン (:) 、アスタリスク (*) 、疑問符 (?) 、左かぎかっこ (<) 、右かぎかっこ (>) 、縦棒 (|) 、クオーテーションマーク(") 、またはアット記号 (@) です。このオプションを指定しない場合、マッピングに名前はありません。

priority *priority*: マッピングのプライオリティを 0~2147483647 の範囲で指定します。値が小さいほど、優先順位が高くなります。このオプションを指定しない場合、マッピングのプライオリティは同じタイプの NAT 規則の中で最も低くなります。

disable: net-to-net 送信スタティックマッピングを無効にします。このキーワードを指定しない場合、マッピングは有効になります。

counting: NAT カウントを有効にします。アドレスマッピングを使用するフローの数がカウントされます。

説明

nat static outbound net-to-net コマンドは送信スタティック NAT の net-to-net マッピングを設定します。

undo nat static outbound net-to-net コマンドは送信スタティック NAT の net-to-net マッピングを削除します。

開始アドレスと終了アドレスでプライベートネットワークを指定し、パブリックアドレスとマスクでパブリックネットワークを指定します。

内部ネットワークからのパケットの送信元アドレスがプライベートアドレス範囲と一致する場合、送信元アドレスはパブリックアドレス範囲内のパブリックアドレスに変換されます。外部ネットワークからのパケットの宛先アドレスがパブリックアドレス範囲と一致する場合、宛先アドレスはプライベートアドレス範囲内のプライベートアドレスに変換されます。

プライベート終了アドレスは、プライベート開始アドレスとパブリックネットワークマスクによって決定されるサブネット内の最大 IP アドレスより大きくすることはできません。たとえば、パブリックアドレスは 2.2.2.0、マスクは 255.255.255.0、プライベート開始アドレスは 1.1.1.100 です。プライベートエンドアドレスは、サブネット 1.1.1.0/24 内で最大の IP アドレスである 1.1.1.255 を超えることはできません。

ACL を指定する場合は、次の制約事項および注意事項に従ってください。

- ACL を指定しない場合、すべての送信パケットの送信元アドレスとすべての受信パケットの宛先アドレスが変換されます。
- ACL を指定し、reversible キーワードを指定しない場合、ACL によって許可された送信パケットの送信元アドレスが変換されます。外部ネットワークからアクティブに開始された接続の宛先アドレスは、パブリック IP アドレスに変換されません。
- ACL と reversible キーワードの両方を指定すると、ACL によって許可された送信パケットの送信元アドレスが変換されます。外部ネットワークからパブリック IP アドレスに対してアクティブに開始された接続のパケットが ACL リバースマッチングによって許可される場合、宛先アドレスは変換されます。ACL リバースマッチングは次のように機能します。
  - □ パケットの送信元 IP アドレス/ポートと ACL 内の宛先 IP アドレス/ポートを比較します。
  - □ マッピングに従ってパケットの宛先 IP アドレスを変換し、変換された宛先 IP アドレス/ポートを ACL 内の送信元 IP アドレス/ポートと比較します。

スタティック NAT は、両方がインタフェースに設定されている場合、ダイナミック NAT よりも優先されます。

nat static outbound コマンドと nat static outbound net-to-net コマンドを使用すると、複数の送信スタティック NAT マッピングを設定できます。

同じプライオリティ値と ACL で設定された送信スタティック NAT のネット/ネットマッピングは、マッピングで ACL を使用して照合されます。

- 名前付き ACL を持つマッピングは、名前なし ACL を持つマッピングよりも優先順位が高くなります。
- 名前付き ACL を持つマッピングは、ACL 名のアルファベット順に一致します。
- 名前なし ACL を持つマッピングは、ACL 番号の降順で照合されます。

例

#プライベートネットワークアドレス 192.168.1.0/24 とパブリックネットワークアドレス 2.2.2.0/24 の間の送信スタティック NAT マッピングを設定します。

<AP> system-view

[AP] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24

#送信スタティック NAT を設定します。サブネット 192.168.1.0/24 の内部ユーザが、サブネット 2.2.2.0/24 のパブリック IP アドレスを使用して外部サブネット 3.3.3.0/24 にアクセスできるようにします。

<AP> system-view

[AP] acl advanced 3001

[AP-acl-ipv4-adv-3001] rule permit ip destination 3.3.3.0 0.0.0.255

[AP-acl-ipv4-adv-3001] quit

[AP] nat static outbound net-to-net 192.168.1.1 192.168.1.255 global 2.2.2.0 24 acl 3001

関連コマンド

- **display nat all**
- **display nat static**
- **nat static enable**

11.1.32 nat static outbound rule move

Syntax

nat static outbound rule move *nat-rule-name1* { **after** | **before** } *nat-rule-name2*

View

System view

定義済みユーザロール

network-admin

パラメータ

nat-rule-name1: 移動する NAT ルールの名前を指定します。

after: ルール nat-rule-name 1 をルール nat-rule-name 2 の後の行 (参照ルールと呼ばれます) に移動します。参照規則の優先度の値は変更されません。移動されたルールの優先度の値は、参照ルールの優先度の値に 1 を加えた値と等しくなります。

before: ルール nat-rule-name 1 をルール nat-rule-name 2 の前の行に移動します。参照規則の優先度の値は変更されません。移動したルールの優先度値は、参照ルールの優先度値から 1 を引いた値と等しくなります。

nat-rule-name2: 移動する NAT 規則の参照規則として、NAT 規則の名前を指定します。

説明

nat static outbound rule move コマンドは送信 1 対 1 スタティック NAT ルールのプライオリティを変更します。

このコマンドは、名前付き送信 1 対 1 スタティック NAT ルールだけに適用されます。

ルールリストの前の方に表示されている NAT ルールは、パケットマッチングの優先順位が高くなります。

例

#送信 1 対 1 スタティック NAT ルール abc を、送信 1 対 1 スタティック NAT ルール def の前の行に移動します。

<AP> system-view

[AP] nat static outbound rule move abc before def

関連コマンド

nat static outbound

11.1.33 reset nat count statistics

Syntax

reset nat count statistics { **all** | **dynamic** | **server** | **static** | **static-port-block** }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: NAT マッピングのすべてのカウント統計情報をクリアします。

dynamic: ダイナミック NAT マッピングのカウント統計情報をクリアします。

server: NAT サーバマッピングのカウント統計情報をクリアします。

static: スタティック NAT マッピングのカウント統計情報をクリアします。

static-port-block: NAT 444 マッピングのカウント統計情報をクリアします。

説明

reset nat count statistics コマンドは NAT カウント統計情報を削除します。

例

#スタティック NAT マッピングのすべてのカウント統計情報をクリアします。

<AP> reset nat count statistics all

関連コマンド

display nat inbound

display nat outbound

display nat outbound port-block-group

display nat port-block

display nat static

display nat server

11.1.34 reset nat session

Syntax

reset nat session

View

User view

定義済みユーザロール

network-admin

説明

reset nat session コマンドは NAT セッションを削除します。

NAT セッションをクリアすると、対応する NAT EIM テーブルと NO-PAT テーブルが同時にクリアされます。

例

すべての NAT セッションをクリアします。

<AP> reset nat session

関連コマンド

display nat session

目次

このセクションのページは **4-x-x** です。

12 章 IP パフォーマンスの最適化 12-1
12.1 IP パフォーマンスの最適化設定コマンド 12-1
12.1.1 display icmp statistics 12-1
12.1.2 display ip statistics 12-2
12.1.3 display rawip 12-4
12.1.4 display rawip verbose 12-5
12.1.5 display tcp 12-11
12.1.6 display tcp statistics 12-12
12.1.7 display tcp verbose 12-15
12.1.8 display udp 12-23
12.1.9 display udp statistics 12-24
12.1.10 display udp verbose 12-25
12.1.11 ip forward-broadcast 12-30
12.1.12 ip icmp error-interval 12-31
12.1.13 ip mtu 12-32
12.1.14 ip redirects enable 12-33
12.1.15 ip ttl-expires enable 12-34
12.1.16 ip unreachables enable 12-35
12.1.17 reset ip statistics 12-36
12.1.18 reset tcp statistics 12-37
12.1.19 reset udp statistics 12-38
12.1.20 tcp path-mtu-discovery 12-38
12.1.21 tcp timer fin-timeout 12-39
12.1.22 tcp timer syn-timeout 12-41
12.1.23 tcp window 12-41

12章 IP パフォーマンスの最適化

12.1 IPパフォーマンスの最適化設定コマンド

12.1.1 display icmp statistics

Syntax

display icmp statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display icmp statistics コマンドは ICMP パケットの送受信に関する統計情報を表示します。

例

ICMP の統計情報を表示します。

<AP> display icmp statistics

```
  Input: bad formats   0               bad checksum             0
        echo           175             destination unreachable  0
        source quench  0               redirects                0
        echo replies   201             parameter problem        0
        timestamp      0               information requests     0
        mask requests  0               mask replies             0
        time exceeded  0               invalid type             0
        router advert  0               router solicit           0
        broadcast/multicast echo requests ignored          0
        broadcast/multicast timestamp requests ignored     0
 Output: echo         0              destination unreachable  0
        source quench 0               redirects             0
        echo replies  175             parameter problem     0
        timestamp     0               information replies   0
        mask requests 0               mask replies          0
        time exceeded 0               bad address           0
        packet error  1442            router advert         3
```

12.1.2 display ip statistics

Syntax

display ip statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip statistics コマンドは IP パケットの統計情報を表示します。

IP 統計情報はパケットの送受信、再構築に関する情報が含まれます。

例

IP パケットの統計情報を表示します。

<AP> display ip statistics

```
Input:   sum           7120          local           112
         bad protocol   0            bad format      0
         bad checksum   0            bad options     0
         dropped        0
Output:  forwarding     0            local           27
         dropped        0            no route        2
         compress fails 0
Fragment:input          0            output          0
         dropped        0
         fragmented     0            couldn't fragment 0
Reassembling:sum        0            timeouts        0
```

表 12-1 コマンド出力

フィールド	説明
Input	受信したパケットの統計情報です。 • **sum**–受信したパケットの総数です。 • **local**–装置へ送信されたパケットの総数です。 • **bad protocol**–不明なプロトコルのパケットの総数です。 • **bad format**–不正なフォーマットのパケットの総数です。 • **bad checksum**–不正なチェックサムのパケットの総数です。

フィールド	説明
	• **bad options**–不正なオプションのパケットの総数です。
Reassembling	リアセンブルパケットの統計情報です。 • **fragments**–リアセンブルが必要なフラグメントの総数です。 • **reassembled**–リアセンブルされたパケットの総数です。 • **dropped**–リアセンブルに失敗してドロップされたフラグメントの総数です。 • **timeouts**–リアセンブリタイムアウトの総数です。
Fragment	フラグメントパケットの統計情報です。 • **fragmented**–正常にフラグメントされたパケットの総数です。 • **couldn't fragment**–フラグメントに失敗したパケットの総数です。 • **output**–送信したフラグメントパケットの総数です。
Forwarded Frags	転送されたフラグメントに関する統計情報です。 • **sum**–直接転送されたフラグメントの合計数です。

関連コマンド

- **display ip interface**
- **reset ip statistics**

12.1.3 display rawip

Syntax

display rawip

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display rawip コマンドは RawIP 接続の概要情報を表示します。

RawIP 接続の概要情報はローカルアドレス、ピアのアドレス、プロトコル、PCB が含まれます。

例

RawIP 接続の概要情報を表示します。

<AP> display rawip

```
Local Addr      Foreign Addr    Protocol    Cpu PCB
0.0.0.0         0.0.0.0         1           0   0x0000000000000009
0.0.0.0         0.0.0.0         1           0   0x0000000000000008
0.0.0.0         0.0.0.0         1           0   0x0000000000000002
```

表 12-2 コマンド出力

フィールド	説明
Local Addr	ローカルIPアドレスです。
Foreign Addr	ピアのIPアドレスです。
Protocol	プロトコル番号です。
PCB	プロトコルコントロールブロックです。

12.1.4 display rawip verbose

Syntax

display rawip verbose [**pcb** *pcb-index*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の RawIP 接続の詳細情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 16 進数で 1～ffffffffffffffff です。

説明

display rawip verbose コマンドは RawIP 接続の詳細情報を表示します。

RawIP 接続の詳細情報はソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、RawIP 接続の送信元 IP アドレス、RawIP 接続の宛先 IP アドレスが含まれます。

例

RawIP 接続の詳細情報を表示します。

<AP> display rawip verbose

```
Total RawIP socket number: 1

 Creator: ping[320]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 9216 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 3
 Protocol: 1
 Connection info: src = 0.0.0.0, dst = 0.0.0.0
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
```

```
Receive VRF: 0xffff
```

表 12-3 コマンド出力

フィールド	説明
Total RawIP socket number	RawIPソケットの総数です。
Connection info	送信元IPアドレスと宛先IPアドレスを含む接続情報です。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。 • **NOFDREF**–ユーザが接続を閉じました。 • **ISCONNECTED**–接続が確立されました。 • **ISCONNECTING**–接続が確立されています。 • **ISDISCONNECTING**–接続が中断されています。 • **ISSMOOTHING**–クロスカードデータスムージングが進行中です。 • **CANBIND**–ソケットはバインド操作をサポートします。 • **ASYNC**–非同期モード。 • **ISDISCONNECTED**–接続が終了しました。 • **PROTOREF**–強力なプロトコル参照を示します。 • **ISPCBSYNCING**–クロスカードPCB同期が進行中です。 • **N/A**–上記のいずれの状態でもありません。
Options	ソケットのオプションです。 • **SO_DEBUG**–ソケットのデバッグ情報を記録します。 • **SO_ACCEPTCONN**–サーバが接続要求をリッスンできるようにします。 • **SO_REUSEADDR**–ローカルアドレスの再利用を許可します。 • **SO_KEEPALIVE**–接続がまだ有効かどうかをテストするプロトコルを要求します。 • **SO_DONTROUTE**–宛先が直接接続されたネットワーク内にあるため、発信パケットのルーティングテーブルクエリーをバイパスします。 • **SO_BROADCAST**–ブロードキャストパケットをサポートします。 • **SO_LINGER**–ソケットを閉じます。システムは、ソケット送信バッファ内の残りのデータを送信できます。 • **SO_OOBINLINE**–アウトオブバンドデータを入力キューに格納します。

フィールド	説明
	• **SO_REUSEPORT**–ローカルポートの再利用を許可します。 • **SO_TIMESTAMP**–着信パケットのタイムスタンプをミリ秒単位で記録します。このオプションは、接続指向ではないプロトコルに適用できます。 • **SO_NOSIGPIPE**–ソケットからのデータ送信を無効にします。そのため、リターンエラーが発生したときにシグパイプを確立できません。 • **SO_FILTER**–パケットフィルタ基準の設定をサポートします。このオプションは、着信パケットに対して有効になります。 • **SO_TIMESTAMPNS**–ナノ秒まで正確なタイムスタンプと同様の機能があります。 • **SO_SEQPACKET**–ソケットバッファに送信されるパケットの境界を保持します。 • **SO_FILLTWAMPTIME**–TWAMPのタイムスタンプを設定します。 • **SO_LOCAL**–ローカルソケットオプション。 • **SO_DONTDELIVER**–アプリケーションにデータを配信しません。 • **N/A**–上記のいずれの状態でもありません。
Error	エラーコードです。
Receiving buffer (cc/hiwat/lowat/drop/state)	以下の順番で受信バッファ情報を表示します。 • **cc**–使用されているバッファ空間です。 • **hiwat**–最大バッファ空間です。 • **lowat**–最小バッファ空間です。 • **drop**–パケット廃棄数です。 • **state**–バッファ状態です。 　• **CANTSENDMORE**–ピアにデータを送信できません。 　• **CANTRCVMORE**–ピアからデータを受信できません。 　• **RCVATMARK**–タグを受信しています。 　• **N/A**–上記以外の状態です。
Sending buffer (cc/hiwat/lowat/state)	以下の順番で送信バッファ情報を表示します。 • **cc**–使用されているバッファ空間です。 • **hiwat**–最大バッファ空間です。 • **lowat**–最小バッファ空間です。 • **state**–バッファ状態です。 　• **CANTSENDMORE**–ピアにデータを送信できません。

フィールド	説明
	• **CANTRCVMORE**–ピアからデータを受信できません。 • **RCVATMARK**–タグを受信しています。 • **N/A**–上記以外の状態です。
Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。
Inpcb flags	インタネットPCBのフラグです。 • **INP_RECVOPTS**–IPオプションを受信します。 • **INP_RECVRETOPTS**–応答したIPオプションを受信します。 • **INP_RECVDSTADDR**–宛先IPアドレスを受信します。 • **INP_HDRINCL**–全体のIPヘッダを提供します。 • **INP_REUSEADDR**–IPアドレスを再利用します。 • **INP_REUSEPORT**–ポート番号を再利用します。 • **INP_ANONPORT**–ポート番号が指定されていません。 • **INP_RECVIF**–パケットの入力インタフェースを記録します。 • **INP_RECVTTL**–パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_DONTFRAG**–DF(Don't Fragment)フラグを設定します。 • **INP_ROUTER_ALERT**–ルータ警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 • **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 • **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 • **INP_SNDBYLSPV–VPN**--インスタンスを通して送信します。 • **INP_RECVTOS**–パケットのTOSを受信します。このフラグ

フィールド	説明
	はUDPとRawIPのみサポートします。 • **INP_USEICMPSRC**–送信ICMPパケットの送信元IPアドレスとして指定したIPアドレスを使用します。 • **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 • **INP_LOCAL**–同じカード上のこのフラグを持つINPCBと優先的に一致します。 • **N/A**–上記以外のフラグです。
Inpcb extflag	インタネットPCBの拡張フラグです。 • **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスの記録です。 • **INP_RCVPWID**–受信したパケットのPW IDの記録です。 • **INP_EXTRCVICMPERR**–ICMPエラーパケットを受信します。 • **INP_EXTFILTER**–受信したパケットの内容をフィルタリングします。 • **INP_EXTDONTDROP**–受信したパケットをドロップしません。 • **INP_EXLISTEN**–このフラグを持つINPCBをリッスンハッシュテーブルに追加します。 • **INP_SELECTMATCHSRCBYFIB**–FIBテーブルを使用して、一致するソースを選択します。 • **INP_EXTPRIVATESOCKET**–INPCBをNSRプライベートソケットに関連付けます。 • **INP_EXLISTENNET**:接続情報がネットワークセグメントリンクリストに追加されたときに、このフラグを設定します。 • **N/A**–上記以外のフラグです。
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 • **INP_IPV4**–IPv4プロトコルです。 • **INP_TIMEWAIT**–TIMEWAIT状態です。 • **INP_ONESBCAST**–ブロードキャストパケットを送信します。 • **INP_DROPPED**–プロトコルがフラグを廃棄しました。 • **INP_SOCKREF**–Strongソケットを参照します。 • **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 • **N/A**–上記以外のフラグです。

フィールド	説明
TTL	インタネットPCBのTTLです。
Send VRF	パケットの送信元となるVRFです。
Receive VRF	パケットの受信元となるVRFです。

12.1.5 display tcp

Syntax

display tcp

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display tcp コマンドは TCP 接続の概要情報を表示します。

TCP 接続の概要情報はローカル IP アドレス、ローカルポート番号、ピアの IP アドレス、ピアのポート番号、TCP 接続情報が含まれます。

例

TCP 接続の概要情報を表示します。

<AP> display tcp

```
 *: TCP connection with authentication
 Local Addr:port    Foreign Addr:port     State       Cpu PCB
*0.0.0.0:21         0.0.0.0:0             LISTEN      0  0x000000000000c387
 192.168.20.200:23  192.168.20.14:1284    ESTABLISHED 0  0x0000000000000009
 192.168.20.200:23  192.168.20.14:1283    ESTABLISHED 0  0x0000000000000002
```

表 12-4 コマンド出力

フィールド	説明
*	TCP接続が認証を使用することを示します。
Local Addr:port	ローカルIPアドレスとポート番号です。
Foreign Addr:port	ピアのIPアドレスとポート番号です。
State	TCP接続状態です。
PCB	PCBインデックスです。

12.1.6 display tcp statistics

Syntax

display tcp statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display tcp statistics コマンドは TCP トラフィックの統計情報を表示します。

TCP トラフィックの統計情報は受信 TCP パケット、送信 TCP パケット、Syncache/syncookie が含まれます。

例

TCP トラフィックの統計情報を表示します。

<AP> display tcp statistics

```
Received packets:
   Total: 4150
   packets in sequence: 1366 (134675 bytes)
   window probe packets: 0, window update packets: 0
   checksum error: 0, offset error: 0, short error: 0
   packets dropped for lack of memory: 0
   packets dropped due to PAWS: 0
   duplicate packets: 12 (36 bytes), partially duplicate packets: 0 (0 bytes)
   out-of-order packets: 0 (0 bytes)
   packets with data after window: 0 (0 bytes)
   packets after close: 0
   ACK packets: 3531 (795048 bytes)
   duplicate ACK packets: 33, ACK packets for unsent data: 0

Sent packets:
   Total: 4058
   urgent packets: 0
   control packets: 50
   window probe packets: 3, window update packets: 11
   data packets: 3862 (795012 bytes), data packets retransmitted: 0 (0 bytes)
   ACK-only packets: 150 (52 delayed)
   unnecessary packet retransmissions: 0
```

```
Syncache/syncookie related statistics:
    entries added to syncache: 12
    syncache entries retransmitted: 0
    duplicate SYN packets: 0
    reply failures: 0
    successfully build new socket: 12
    bucket overflows: 0
    zone failures: 0
    syncache entries removed due to RST: 0
    syncache entries removed due to timed out: 0
    ACK checked by syncache or syncookie failures: 0
    syncache entries aborted: 0
    syncache entries removed due to bad ACK: 0
    syncache entries removed due to ICMP unreachable: 0
    SYN cookies sent: 0
    SYN cookies received: 0

SACK related statistics:
    SACK recoveries: 1
    SACK retransmitted segments: 0 (0 bytes)
    SACK blocks (options) received: 0
    SACK blocks (options) sent: 0
    SACK scoreboard overflows: 0

Other statistics:
    retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
    persist timeout: 0
    keepalive timeout: 21, keepalive probe: 0
    keepalive timeout, so connections disconnected: 0
    fin_wait_2 timeout, so connections disconnected: 0
    initiated connections: 29, accepted connections: 12, established connections:
23
    closed connections: 50051 (dropped: 0, initiated dropped: 0)
    bad connection attempt: 0
    ignored RSTs in the window: 0
    listen queue overflows: 0
    RTT updates: 3518(attempt segment: 3537)
    correct ACK header predictions: 0
    correct data packet header predictions: 568
    resends due to MTU discovery: 0
    packets dropped with MD5 authentication: 0
    packets permitted with MD5 authentication: 0
```

関連コマンド

reset tcp statistics

12.1.7 display tcp verbose

Syntax

display tcp verbose [**pcb** *pcb-index*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の TCP 接続の詳細情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 16 進数で 1～ffffffffffffffff です。

説明

display tcp verbose コマンドは TCP 接続の詳細情報を表示します。

TCP 接続の詳細情報はソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号、接続状態が含まれます。

例

TCP 接続の詳細情報を表示します。

<AP> display tcp verbose

```
TCP inpcb number: 1(tcpcb number: 1)

 NSR standby: N/A
 Creator: bgpd[199]
 State: ISCONNECTED
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat /drop/state): 0 / 65700 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 65700 / 512 / N/A
 Type: 1
 Protocol: 6
 Connection info: src = 192.168.20.200:179 ,  dst = 192.168.20.14:4181
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
```

```
Connection state: ESTABLISHED
TCP options: TF_REQ_SCALE TF_REQ_TSTMP TF_SACK_PERMIT TF_NSR
NSR state: READY(M)
Send VRF: 0x0
Receive VRF: 0x0
```

表 12-5 コマンド出力

フィールド	説明
TCP inpcb number	TCP IP PCBの数です。
Connection info	送信元IPアドレス、送信元ポート番号、宛先IPアドレス、宛先ポート番号などの接続情報です。
tcpcb number	TCP PCBの数です。TCP接続の状態がTIME_WAITの場合、このフィールドは表示されません。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。 • **NOFDREF**–ユーザは接続を閉じました。 • **ISCONNECTED**–接続が確立されました。 • **ISSMOOTHING**–クロスカードデータスムージングが進行中です。 • **CANBIND**–ソケットはバインド操作をサポートします。 • **ISCONNECTING**–接続を確立中です。 • **ISDISCONNECTING**–接続を中断中です。 • **ASYNC**–非同期モード。 • **ISDISCONNECTED**–接続が終了しました。 • **PROTOREF**–強力なプロトコル参照を示します。 • **ISPCBSYNCING**–クロスカードPCB同期が進行中です。 • **N/A**–上記のいずれの状態でもありません。
Options	ソケットのオプションです。 • **SO_DEBUG**–ソケットのデバッグ情報を記録します。 • **SO_ACCEPTCONN**–サーバが接続要求をリッスンできるようにします。 • **SO_REUSEADDR**–ローカルアドレスの再利用を許可します。 • **SO_KEEPALIVE**–接続がまだ生きているかどうかをテストするためにプロトコルを必要とします。 • **SO_DONTROUTE**–宛先が直接接続されたネットワーク内にあるため、発信パケットのルーティングテーブルクエリーをバイパスします。 • **SO_BROADCAST**–ブロードキャストパケットをサポート

フィールド	説明
	します。 • **SO_LINGER**–ソケットを閉じます。システムは、ソケット送信バッファ内の残りのデータを送信できます。 • **SO_OOBINLINE**–アウトオブバンドデータを入力キューに格納します。 • **SO_REUSEPORT**–ローカルポートの再利用を許可します。 • **SO_TIMESTAMP**–着信パケットのタイムスタンプをミリ秒単位で記録します。このオプションは、接続指向ではないプロトコルに適用できます。 • **SO_NOSIGPIPE**–ソケットからのデータ送信を無効にします。そのため、リターンエラーが発生したときにシグパイプを確立できません。 • **SO_TIMESTAMPNS**–ナノ秒まで正確なタイムスタンプと同様の機能を持っています。 • **SO_KEEPALIVETIME**–キープアライブ時間を設定します。 • **SO_SEQPACKET**–ソケットバッファに送信されたパケットの境界を保持します。 • **SO_USCBINDEX**–受信パケットからユーザプロファイルインデックスを取得します。 • **SO_FILLTWAMPTIME**–TWAMPのタイムスタンプを設定します。 • **SO_LOCAL**–ローカルソケットオプション。 • **SO_DONTDELIVER**–アプリケーションにデータを配信しません。 • **N/A**–オプションは設定されていません。
Error	エラーコードです。

Receiving buffer
(cc/hiwat/lowat/state)
	以下の順番で受信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Sending buffer (cc/hiwat/lowat/state)	以下の順番で送信バッファ情報を表示します。 • **cc**–使用されているバッファ空間です。

フィールド	説明

	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。
Inpcb flags	インタネットPCBのフラグです。 • **INP_RECVOPTS**–IPオプションを受信します。 • **INP_RECVRETOPTS**–応答したIPオプションを受信します。 • **INP_RECVDSTADDR**–宛先IPアドレスを受信します。 • **INP_HDRINCL**–IPヘッダ全体を提供します。 • **INP_REUSEADDR**–IPアドレスを再利用します。 • **INP_REUSEPORT**–ポート番号を再利用します。 • **INP_ANONPORT**–ポート番号が指定されていません。 • **INP_RECVIF**–パケットの入力インタフェースを記録します。 • **INP_RECVTTL**–パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_DONTFRAG**–DF(Don't Fragment)フラグを設定します。 • **INP_ROUTER_ALERT**–ルータで警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 • **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 • **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。

フィールド	説明
	• **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 • **INP_SNDBYLSPV–VPN**–インスタンスを通して送信します。 • **INP_RECVTOS**–パケットのTOSを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 • **N/A**–上記以外のフラグです。
Inpcb extflag	インタネットPCBの拡張フラグです。 • **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスを記録します。 • **INP_RCVPWID**–受信したパケットのPW IDを記録します。 • **INP_EXTDONTDROP**–受信したパケットを廃棄しません。 • **N/A**–上記以外のフラグです。
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 • **INP_IPV4**–IPv4プロトコルです。 • **INP_TIMEWAIT**–TIMEWAIT状態です。 • **INP_ONESBCAST**–ブロードキャストパケットを送信します。 • **INP_DROPPED**–プロトコルがフラグを廃棄しました。 • **INP_SOCKREF**–Strongソケットを参照します。 • **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 • **N/A**–上記以外のフラグです。
TTL	インタネットPCBのTTLです。
TCP options	TCPオプションです。 • **TF_ACKNOW**–ACKパケットをすぐにピアに返します。 • **TF_DELACK**–ACKパケットの送信を遅延します。 • **TF_SENTFIN**–FINパケットが送信されました。 • **TF_RCVD_SCALE**–受信ウィンドウサイズの倍率を要求します。 • **TF_RCVD_TSTMP**–SYNパケットでタイムスタンプを受信しました。 • **TF_NEEDSYN**–SYNパケットを送信します。 • **TF_NEEDFIN**–FINパケットを送信します。 • **TF_MORETOCOME**–ソケットにさらにデータが追加され

フィールド	説明
	ます。 • **TF_LQ_OVERFLOW**–リスニングキューがオーバーフローします。 • **TF_LASTIDLE**–アイドル接続。 • **TF_RXWIN 0 SENT**–受信ウィンドウサイズ0の応答が送信されました。 • **TF_FASTRECOVERY**–NewReno高速回復モードを開始します。 • **TF_WASFRECOVERY**–NewReno高速回復モードの場合。 • **TF_SIGNATURE**–MD5署名を有効にします。 • **TF_FORCEDATA**–強制的に1バイトを送信します。 • **TF_TSO–TSO**を有効にします。 • **TF_PMTU**–RFC 1191をサポートします。 • **TF_PMTUD**–Path MTU discoveryを開始します。 • **TF_PASSIVE_CONN**–パッシブ接続。 • **TF_APP_SEND**–アプリケーションはデータを送信します。 • **TF_NODELAY**–TCP内の送信データをバッファするNagleアルゴリズムを無効にします。 • **TF_NOOPT**–TCPオプションがありません。 • **TF_NOPUSH**–TCPバッファにバッファされるセグメントが満杯になるまでTCPデータの送信を強制的に遅延させます。 • **TF_NSR**–TCP NSRを有効にします。 • **TF_REQ_SCALE**–TCPウィンドウのscaleオプションを有効にします。 • **TF_REQ_TSTMP**–タイムスタンプオプションを有効にします。 • **TF_SACK_PERMIT**–TCP selective acknowledgementオプションを有効にします。 • **TF_ENHANCED_AUTH**–拡張認証オプションを有効にします。
NSR state	TCP接続の状態です。括弧の数は接続の役割です。 • **M**–メイン接続です。 • **S**–Standby接続です。
Send VRF	パケットの送信元となるVRF。
Receive VRF	パケットの受信元となるVRF。

フィールド	説明
Error count in abnormal-packet-defend period	TCP攻撃防止を有効にしてから一定期間内に受信した異常パケット数。
Checksum errors	チェックサムエラーが発生した受信パケット数。
Duplicate packets	重複した受信パケットの数。
Part-Duplicate packets	部分的に重複した受信パケットの数。
Out-of-order packets	シーケンス番号が不正な受信パケットの数。
Duplicate ACK packets	重複して受信されたACKパケットの数。
Out-of-order ACK packets	受信したACKパケットのうち、重複したものの数。Out-of-order ACK packets受信したACKパケットのうち、シーケンス番号が順不同だったものの数
Packets with data out of window	シーケンス番号がスライディングウィンドウになかった受信数。
MD5 authentication errors	MD 5認証エラーが発生したパケットの数。
Keychain authentication errors	キーチェーン認証エラーが発生したパケットの数。
Timestamp errors	タイムスタンプエラーが発生したパケットの数

12.1.8 display udp

Syntax

display udp

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display udp コマンドは UDP 接続の概要情報を表示します。

UDP 接続の概要情報はローカル IP アドレス、ローカルポート番号、ピアの IP アドレス、ピアのポート番号が含まれます。

例

UDP 接続の概要情報を表示します。

<AP> display udp

```
Local Addr:port        Foreign Addr:port    Cpu PCB
0.0.0.0:69             0.0.0.0:0             0   0x0000000000000003
192.168.20.200:1024    192.168.20.14:69      0   0x0000000000000002
```

表 12-6 コマンド出力

フィールド	説明
Local Addr:port	ローカルIPアドレスとポート番号です。
Foreign Addr:port	ピアのIPアドレスとポート番号です。
PCB	PCBインデックスです。

12.1.9 display udp statistics

Syntax

display udp statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display udp statistics コマンドは UDP トラフィックの統計情報を表示します

UDP トラフィックの統計情報は受信 UDP パケット、送信 UDP パケットが含まれます。

例

UDP トラフィックの統計情報を表示します。

<AP> display udp statistics

```
Received packets:
    Total: 240
    checksum error: 0, no checksum: 0
    shorter than header: 0, data length larger than packet: 0
    no socket on port(unicast): 0
    no socket on port(broadcast/multicast): 240
    not delivered, input socket full: 0
Sent packets:
    Total: 0
```

関連コマンド

reset udp statistics

12.1.10 display udp verbose

Syntax

display udp verbose [**pcb** *pcb-index*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

pcb *pcb-index*: 指定した PCB の UDP 接続の詳細情報を表示します。*pcb-index* は PCB のインデックスを指定します。設定範囲は 16 進数で 1～ffffffffffffffff です。

説明

display udp verbose コマンドは UDP 接続の詳細情報を表示します。

UDP 接続の詳細情報は UDP 接続のソケット作成のタスク名、状態、オプション、タイプ、プロトコル番号、送信元 IP アドレス、送信元ポート番号、宛先 IP アドレス、宛先ポート番号が含まれます。

例

UDP 接続の詳細情報を表示します。

<AP> display udp verbose

```
Total UDP socket number: 1


 Creator: sock_test_mips[250]
 State: N/A
 Options: N/A
 Error: 0
 Receiving buffer(cc/hiwat/lowat/drop/state): 0 / 41600 / 1 / 0 / N/A
 Sending buffer(cc/hiwat/lowat/state): 0 / 9216 / 512 / N/A
 Type: 2
 Protocol: 17
 Connection info: src = 0.0.0.0:69, dst = 0.0.0.0:0
 Inpcb flags: N/A
 Inpcb extflag: N/A
 Inpcb vflag: INP_IPV4
 TTL: 255(minimum TTL: 0)
 Send VRF: 0xffff
```

```
Receive VRF: 0xffff
```

表 12-7 コマンド出力

フィールド	説明
Total RawIP socket number	UDPソケットの総数です。
Connection info	送信元IPアドレスと宛先IPアドレスを含む接続情報です。
Creator	ソケットを作成したタスク名です。括弧の数はタスク名の処理番号です。
State	ソケットの状態です。 • **NOFDREF**–ユーザが接続を閉じました。 • **ISCONNECTED**–接続が確立されました。 • **ISCONNECTING**–接続が確立されています。 • **ISDISCONNECTING**–接続が中断されています。 • **ASYNC**–非同期モード。 • **ISDISCONNECTED**–接続が終了しました。 • **ISSMOOTHING**–クロスカードデータスムージングが進行中です。 • **CANBIND**–ソケットはバインド操作をサポートします。 • **PROTOREF**–強力なプロトコル参照を示します。 • **ISPCBSYNCING**–クロスカードPCB同期が進行中です。 • **N/A**–上記のいずれの状態でもありません。
Options	ソケットのオプションです。 • **SO_DEBUG**–ソケットのデバッグ情報を記録します。 • **SO_ACCEPTCONN**–サーバが接続要求をリッスンできるようにします。 • **SO_REUSEADDR**–ローカルアドレスの再利用を許可します。 • **SO_KEEPALIVE**–接続がまだ有効かどうかをテストするプロトコルを要求します。 • **SO_DONTROUTE**–宛先が直接接続されたネットワーク内にあるため、発信パケットのルーティングテーブルクエリーをバイパスします。 • **SO_BROADCAST**–ブロードキャストパケットをサポートします。 • **SO_LINGER**–ソケットを閉じます。システムは、ソケット送信バッファ内の残りのデータを送信できます。 • **SO_OOBINLINE**–アウトオブバンドデータを入力キューに格納します。

フィールド	説明
	• **SO_REUSEPORT**–ローカルポートの再利用を許可します。 • **SO_TIMESTAMP**–着信パケットのタイムスタンプをミリ秒単位で記録します。このオプションは、接続指向ではないプロトコルに適用できます。 • **SO_NOSIGPIPE**–ソケットからのデータ送信を無効にします。そのため、リターンエラーが発生したときにシグパイプを確立できません。 • **SO_TIMESTAMPNS**–ナノ秒まで正確なタイムスタンプと同様の機能があります。 • **SO_SEQPACKET**–ソケットバッファに送信されるパケットの境界を保持します。 • **SO_USCBINDEX**–受信したパケットからユーザプロファイルインデックスを取得します。 • **SO_FILLTWAMPTIME**–TWAMPのタイムスタンプを設定します。 • **SO_LOCAL**–ローカルソケットオプション。 • **SO_DONTDELIVER**–アプリケーションにデータを配信しません。 • **N/A**–上記のいずれの状態でもありません。
Error	エラーコードです。

Receiving buffer
(cc/hiwat/lowat/drop/state)
	以下の順番で受信バッファ情報を表示します。
	• **cc**–使用されているバッファ空間です。
	• **hiwat**–最大バッファ空間です。
	• **lowat**–最小バッファ空間です。
	• **drop**–パケット廃棄数です。
	• **state**–バッファ状態です。
	  • **CANTSENDMORE**–ピアにデータを送信できません。
	  • **CANTRCVMORE**–ピアからデータを受信できません。
	  • **RCVATMARK**–タグを受信しています。
	  • **N/A**–上記以外の状態です。

Sending buffer (cc/hiwat/lowat/state)	以下の順番で送信バッファ情報を表示します。 • **cc**–使用されているバッファ空間です。 • **hiwat**–最大バッファ空間です。 • **lowat**–最小バッファ空間です。 • **state**–バッファ状態です。 • **CANTSENDMORE**–ピアにデータを送信できません。

フィールド	説明
	• **CANTRCVMORE**–ピアからデータを受信できません。 • **RCVATMARK**–タグを受信しています。 • **N/A**–上記以外の状態です。
Type	ソケットタイプです。 • **1**–SOCK_STREAMです。このソケットはストリームの信頼できる転送を提供するためにTCPを使用します。 • **2**–SOCK_DGRAMです。このソケットはデータグラムの転送を提供するためにUDPを使用します。 • **3**–SOCK_RAWです。このソケットはアプリケーションが次の上位レイヤプロトコルヘッダを変更することを許可します。 • **N/A**–上記以外のタイプです。
Protocol	ソケットを使用したプロトコル数です。
Connection info	送信元IPアドレスと宛先IPアドレスを含む接続情報です。
Inpcb flags	インタネットPCBのフラグです。 • **INP_RECVOPTS**–IPオプションを受信します。 • **INP_RECVRETOPTS**–応答したIPオプションを受信します。 • **INP_RECVDSTADDR**–宛先IPアドレスを受信します。 • **INP_HDRINCL**–全体のIPヘッダを提供します。 • **INP_REUSEADDR**–IPアドレスを再利用します。 • **INP_REUSEPORT**–ポート番号を再利用します。 • **INP_ANONPORT**–ポート番号が指定されていません。 • **INP_RECVIF**–パケットの入力インタフェースを記録します。 • **INP_RECVTTL**–パケットのTTLを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_DONTFRAG**–DF(Don't Fragment)フラグを設定します。 • **INP_ROUTER_ALERT**–ルータ警告オプションのパケットを受信します。このフラグはRawIPのみサポートします。 • **INP_PROTOCOL_PACKET**–プロトコルパケットを識別します。 • **INP_RCVVLANID**–パケットのVLAN IDを受信します。このフラグはUDPとRawIPのみサポートします。 • **INP_RCVMACADDR**–フレームのMACアドレスを受信します。 • **INP_RECVTOS**–パケットのTOSを受信します。このフラグ

フィールド	説明
	はUDPとRawIPのみサポートします。 • **INP_SYNCPCB**–インタネットPCBが同期されるまで待ちます。 • **INP_LOCAL**–同じカード上のこのフラグを持つINPCBと優先的に一致します。 • **N/A**–上記以外のフラグです。
Inpcb extflag	インタネットPCBの拡張フラグです。 • **INP_EXTRCVPVCIDX**–受信したパケットのPVCインデックスの記録です。 • **INP_RCVPWID**–受信したパケットのPW IDの記録です。 • **INP_EXTRCVICMPERR**–ICMPエラーパケットを受信します。 • **INP_EXTFILTER**–受信したパケットの内容をフィルタリングします。 • **INP_EXTDONTDROP**–受信したパケットをドロップしません。 • **INP_EXLISTEN**–このフラグを持つINPCBをリッスンハッシュテーブルに追加します。 • **INP_SELECTMATCHSRCBYFIB**–FIBテーブルを使用して、一致するソースを選択します。 • **INP_EXTPRIVATESOCKET**–INPCBをNSRプライベートソケットに関連付けます。 • **INP_EXLISTENNET**–接続情報がネットワークセグメントリンクリストに追加されたときに、このフラグを設定します。 • **N/A**–上記以外のフラグです。
Inpcb vflag	インタネットPCBのIPバージョンフラグです。 • **INP_IPV4**–IPv4プロトコルです。 • **INP_TIMEWAIT**–TIMEWAIT状態です。 • **INP_ONESBCAST**–ブロードキャストパケットを送信します。 • **INP_DROPPED**–プロトコルがフラグを廃棄しました。 • **INP_SOCKREF**–Strongソケットを参照します。 • **INP_DONTBLOCK**–インタネットPCBの同期をブロックしません。 • **N/A**–上記以外のフラグです。
TTL	インタネットPCBのTTLです。

フィールド	説明
Send VRF	パケットの送信元となるVRFです。
Receive VRF	パケットの受信元となるVRFです。

12.1.11 ip forward-broadcast

Syntax

ip forward-broadcast

undo ip forward-broadcast

デフォルト

無効

View

Interface view

定義済みユーザロール

network-admin

説明

ip forward-broadcast コマンドは直接接続されたネットワークにダイレクトブロードキャストパケットの送受信をインタフェースで有効にします。

undo ip forward-broadcast コマンドは直接接続されたネットワークにダイレクトブロードキャストパケットの送受信をインタフェースで無効にします。

ダイレクトブロードキャストパケットは指定したネットワークのすべてのホストに送信されるブロードキャストパケットのことです。ダイレクトブロードキャストパケットの宛先 IP アドレスのネットワーク ID は宛先ネットワークを識別し、ホスト ID は値がすべて 1 です。

インタフェースが、ダイレクトブロードキャストをネットワークに転送することを許可した場合、ハッカーがネットワークに攻撃をする可能性があります。

例

直接接続されたネットワークにダイレクトブロードキャストパケットの送受信を VLAN インタフェース 2 で有効にします。

<AP> system-view

[AP] interface vlan-interface 2

[AP-Vlan-interface2] ip forward-broadcast

12.1.12 ip icmp error-interval

Syntax

ip icmp error-interval *interval* [*bucketsize*]

undo ip icmp error-interval

デフォルト

最大バケットサイズは最大 10 トークンで、バケットに 100 ミリ秒の間隔でトークンが配置されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: バケットに到着するトークンの間隔を設定します。設定範囲は 0～2147483647 です。ICMP レートリミットを無効にする場合 0 に設定します。

bucketsize: 最大トークンバケットサイズを指定します。設定範囲は 1～200 です。

説明

ip icmp error-interval コマンドは ICMP エラーメッセージがトークンバケット（bucket）に到着する間隔と、トークンパケットサイズを設定します。つまり ICMP レートリミットを設定します。

undo ip icmp error-interval コマンドはデフォルトに戻します。

このコマンドは ICMP エラーメッセージが送信されるレートを制限します。このコマンドを使用することで、ネットワークの衝突が発生する可能性のある短い時間内に過度の ICMP エラーメッセージを送信することを防ぐことができます。トークンバケットアルゴリズムは 1 つの ICMP エラーメッセージを表す 1 つのトークンが用いられます。

バケットに入ることができるトークンが最大に到達するまでトークンは指定された間隔でバケットに配置されます。

ICMP エラーメッセージが送信されるとき、バケットからトークンがバケットから取り除かれます。バケットが空の時、新しいトークンがバケットに配置されるまで ICMP エラーメッセージは送信されません。

例

ICMP エラーメッセージの送信間隔を 200 ミリ秒、トークンのバケットサイズを 40 に設定します。

<AP> system-view

[AP] ip icmp error-interval 200 40

12.1.13 ip mtu

Syntax

ip mtu *mtu-size*

undo ip mtu

デフォルト

設定なし

View

Interface view

定義済みユーザロール

network-admin

パラメータ

mtu-size: MTU を指定します。設定範囲は 128～1587 バイトです。

説明

ip mtu コマンドはインタフェースを通過する IPv4 パケットの MTU を設定します。

undo ip mtu コマンドはデフォルトに戻します。

出力インタフェースの MTU を超過したとき、装置は以下のどちらか 1 つを処理します。

- パケットのフラグメントが禁止されている場合、装置はパケットを廃棄します。
- パケットのフラグメントが許可されている場合、装置はパケットを分割し、フラグメントしたパケットを転送します。

フラグメントと再構築は、システムリソースを消費します。フラグメントを防ぐため、ネットワーク環境にもとづいて、適切にインタフェースの MTU サイズを設定します。

例

VLAN インタフェース 100 の MTU を 1280 バイトに設定します。

<AP> system-view

[AP] interface vlan-interface 100

[AP-Vlan-interface100] ip mtu 1280

12.1.14 ip redirects enable

Syntax

ip redirects enable

undo ip redirects enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip redirects enable コマンドは ICMP リダイレクトメッセージの送信を有効にします。

undo ip redirects enable コマンドは ICMP リダイレクトメッセージの送信を無効にします。

ICMP リダイレクトパケット機能はホストの管理を簡略化し、最適なルートを見つけ出すために、ホストが正しいルーティングテーブルを徐々に確立することができます。

ホストはすべてのパケットをデフォルトゲートウェイに送信するため、デフォルトルートへのルートのみがあります。デフォルトゲートウェイは、以降のパケットを送信するために正しいネクストホップを再選択するよう、以下の条件で、送信元の装置に ICMP リダイレクトパケットを送信します。

- 受信インタフェースと送信インタフェースが同じです。
- 選択したルートが ICMP リダイレクトパケットで作成されていない、あるいは変更されていません。
- 選択されたルートが 0.0.0.0 へのルートではありません。
- 受信したパケットに送信元ルートオプションがありません。

例

ICMP リダイレクトメッセージの送信を有効にします。

<AP> system-view

[AP] ip redirects enable

12.1.15 ip ttl-expires enable

Syntax

ip ttl-expires enable

undo ip ttl-expires enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip ttl-expires enable コマンドは ICMP タイムアウトパケットの送信を有効にします。

undo ip ttl-expires enable コマンドは ICMP タイムアウトパケットの送信を無効にします。

装置は以下のルールによって ICMP タイムアウトパケットを送信します。

- パケットの宛先が装置自身ではなく、パケットの TTL フィールドが 1 であるとき、装置は以下の状態の場合、送信元に ICMP TTL Expired の ICMP エラーパケットを送信します。
  - □ パケットの宛先が装置自身ではありません。
  - □ パケットの TTL フィールドが 1 です。
- 宛先が装置自身である IP データグラムの最初のフラグメントパケットを、装置が受信したとき、タイマを始動します。データグラムのすべてのフラグメントパケットを受信する前にタイマが満了した場合、装置は ICMP Fragment Reassembly Timeout の ICMP エラーパケットを送信します。

ICMP タイムアウトパケットの送信を無効にした装置は ICMP TTL Expired の ICMP エラーパケットを送信しませんが、ICMP Fragment Reassembly Timeout のメッセージを送信します。

例

ICMP タイムアウトパケットの送信を有効にします。

<AP> system-view

[AP] ip ttl-expires enable

12.1.16 ip unreachables enable

Syntax

ip unreachables enable

undo ip unreachables enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ip unreachables enable コマンドは ICMP 宛先到達不能メッセージの送信を有効にします。

undo ip unreachables enable コマンドは ICMP 宛先到達不能メッセージの送信を無効にします。

装置は以下のルールで宛先到達不能メッセージを送信します。

- 以下の状態の場合、装置は Network Unreachable の ICMP エラーパケットを送信元に送信します。
  - 受信したパケットがルートに一致しません。
  - ルーティングテーブルにデフォルトルートがありません。
- 以下の状態の場合、装置は Protocol Unreachable の ICMP エラーパケットを送信元に送信します。
  - 受信したパケットの宛先が装置です。
  - パケットのトランスポート層プロトコルが装置でサポートしていません。
- 以下の状態の場合、装置は ICMP Port Unreachable の ICMP エラーパケットを送信元に送信します。
  - 受信したパケットの宛先が装置です。
  - パケットのポート番号が実行中のプロセスとマッチしません。
- 以下の状態の場合、装置は Source Routing Failure の ICMP エラーパケットを送信元に送信します。
  - パケットを送信するために送信元が、Strict Source Routing を使用しています。
  - 中継装置で、送信元により指定されたネクストホップが直接接続されていないことを検出しました。
- 以下の状態の場合、装置は Fragmentation Needed and Don't Fragment-Set の ICMP エラーパケットを送信元に送信します。
  - 送信インタフェースの MTU がパケットより小さいです。
  - パケットに DF セット(フラグメント禁止)が付与されています。

例

ICMP 宛先到達不能メッセージの送信を有効にします。

<AP> system-view

[AP] ip unreachables enable

12.1.17 reset ip statistics

Syntax

reset ip statistics

View

User view

定義済みユーザロール

network-admin

説明

reset ip statistics コマンドは IP トラフィックの統計情報を削除します。

新しく一定期間内の IP トラフィックの統計情報を取得する場合、このコマンドを使用し、最初に既存の IP トラフィックの統計情報を削除します。

例

IP トラフィックの統計情報を削除します。

<AP> reset ip statistics

関連コマンド

- **display ip interface**
- **display ip statistics**

12.1.18 reset tcp statistics

Syntax

reset tcp statistics

View

User view

定義済みユーザロール

network-admin

説明

reset tcp statistics コマンドは TCP トラフィックの統計情報を削除します。

例

TCP トラフィックの統計情報を削除します。

<AP> reset tcp statistics

関連コマンド

display tcp statistics

12.1.19 reset udp statistics

Syntax

reset udp statistics

View

User view

定義済みユーザロール

network-admin

説明

reset udp statistics コマンドは UDP トラフィックの統計情報を削除します。

例

UDP トラフィックの統計情報を削除します。

<AP> reset udp statistics

関連コマンド

display udp statistics

12.1.20 tcp path-mtu-discovery

Syntax

tcp path-mtu-discovery [**aging** *age-time* | **no-aging**]

undo tcp path-mtu-discovery

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

aging *age-time*: path MTU のエージングタイマを設定します。設定時間は 10～30 分です。デフォルトは 10 分です。

no-aging: path MTU をエージアウトしません。

説明

tcp path-mtu-discovery コマンドは TCP path MTU discovery を有効にします。

undo tcp path-mtu-discovery コマンドは TCP path MTU discovery を無効にします。

TCP path MTU discovery を有効にしたのち、すべての新しい TCP 接続は、path MTU を検出します。装置は IP のフラグメントを発生させないように MSS の計算をするため、path MTU を使用します。

TCP path MTU discovery を無効にしたのち、システムはすべての path MTU タイマを停止します。その後に確立された TCP 接続は path MTU を検出しませんが、以前に確立された TCP 接続は path MTU を検出することができます。

例

TCP path MTU discovery を有効にし、path MTU のエージングタイマを 20 分に設定します。

<AP> system-view

[AP] tcp path-mtu-discovery aging 20

12.1.21 tcp timer fin-timeout

Syntax

tcp timer fin-timeout *time-value*

undo tcp timer fin-timeout

デフォルト

675 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: TCP FIN wait タイマを指定します。設定範囲は 76～3600 秒です。

説明

tcp timer fin-timeout コマンドは TCP FIN wait タイマを設定します。

undo tcp timer fin-timeout コマンドはデフォルトに戻します。

状態が FIN_WAIT_2 に変更したとき、TCP は TCP FIN wait タイマを開始します。時間内に FIN パケットを受信しない場合、TCP 接続が終了します。

FIN パケットを受信した場合、TCP は TIME_WAIT に接続状態を変更します。non-FIN パケットを受信すると、TCP はタイマを再スタートし、TCP はタイマが満了したとき TCP 接続を切断します。

例

TCP FIN wait タイマを 800 秒に設定します。

<AP> system-view

[AP] tcp timer fin-timeout 800

12.1.22 tcp timer syn-timeout

Syntax

tcp timer syn-timeout *time-value*

undo tcp timer syn-timeout

デフォルト

75 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-value: TCP SYN wait タイマを指定します。設定範囲は 2～600 秒です。

説明

tcp timer syn-timeout コマンドは TCP SYN wait タイマを設定します。

undo tcp timer syn-timeout コマンドはデフォルトに戻します。

TCP は SYN パケットを送信した後、SYN wait タイマを開始します。SYN wait タイマの間隔以内にパケットを受信しない場合、TCP は接続の確立に失敗します。

例

TCP SYN wait タイマを 80 秒に設定します。

<AP> system-view

[AP] tcp timer syn-timeout 80

12.1.23 tcp window

Syntax

tcp window *window-size*

undo tcp window

デフォルト

63 KB

View

System view

定義済みユーザロール

network-admin

パラメータ

window-size: TCP 受信/送信バッファのサイズを指定します。設定範囲は 1～64KB です。

説明

tcp window コマンドは TCP 受信/送信バッファのサイズを設定します。

undo tcp window コマンドはデフォルトに戻します。

例

TCP 受信/送信バッファのサイズを 3KB に設定します。

<AP> system-view

[AP] tcp window 3

目次

このセクションのページは **4-x-x** です。

13 章 スタティックルーティング 13-1
13.1 スタティックルーティング設定コマンド 13-1
13.1.1 delete static-routes all 13-1
13.1.2 display ip routing-table 13-1
13.1.3 display ip routing-table acl 13-6
13.1.4 display ip routing-table ip-address 13-9
13.1.5 display ip routing-table prefix-list 13-11
13.1.6 display ip routing-table protocol 13-13
13.1.7 display ip routing-table statistics 13-14
13.1.8 ip route-static 13-15
13.1.9 ip route-static default-preference 13-17
13.1.10 reset ip routing-table statistics protocol 13-17

13章 スタティックルーティング

13.1 スタティックルーティング設定コマンド

13.1.1 delete static-routes all

Syntax

delete static-routes all

View

System view

定義済みユーザロール

network-admin

説明

delete static-routes all コマンドはすべてのスタティックルートを削除します。

コマンドを実行すると、設定されているすべてのスタティックルートを削除する前に確認画面が表示されます。

1 つのスタティックルートを削除する場合、**undo ip route-static** コマンドを使用します。デフォルトルートを含むすべてのスタティックルートを削除する場合、**delete static-routes all** コマンドを使用します。

例

すべてのスタティックルートを削除します。

<AP> system-view

[AP] delete static-routes all

```
This will erase all IPv4 static routes and their configurations, you must
reconfigure all static routes.
Are you sure?[Y/N]:y
```

関連コマンド

ip route-static

13.1.2 display ip routing-table

Syntax

display ip routing-table [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ip routing-table コマンドはルーティングテーブルの情報を表示します。

例

ルーティングテーブルのアクティブルートの概要情報を表示します。

<AP> display ip routing-table

```
Destinations : 12       Routes : 12

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
0.0.0.0/32          Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32        Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
192.168.1.0/24      Direct 0    0           192.168.1.40    Vlan11
192.168.1.0/32      Direct 0    0           192.168.1.40    Vlan11
192.168.1.40/32     Direct 0    0           127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0           192.168.1.40    Vlan11
224.0.0.0/4         Direct 0    0           0.0.0.0         NULL0
224.0.0.0/24        Direct 0    0           0.0.0.0         NULL0
255.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0
```

表 13-1 コマンド出力

フィールド	説明
Destinations	宛先アドレスの数です。
Routes	ルート数です。
Destination/Mask	宛先アドレス/マスク長です。

フィールド	説明
Proto	ルートを指定したプロトコルです。
Pre	ルートの優先順位です。
Cost	ルートのコストです。
NextHop	ルートのネクストホップアドレスです。
Interface	ルートに従って転送されるパケットの出力インタフェースです。
Summary Count	ルート数です。

ルーティングテーブルのすべてのルートの詳細情報を表示します。

<AP> display ip routing-table verbose

```
Destinations : 13       Routes : 13

Destination: 0.0.0.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                Age: 08h34m37s
       Cost: 0            Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1000c       OrigNextHop: 127.0.0.1
      Label: NULL         RealNextHop: 127.0.0.1
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A

Destination: 1.1.1.0/24
   Protocol: Static
 Process ID: 0
  SubProtID: 0x0                Age: 04h20m37s
       Cost: 0            Preference: 60
```

```
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000003        LastAs: 0
     AttrID: 0xffffffff      Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.47.4
      Label: NULL         RealNextHop: 192.168.47.4
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A

...
```

表 13-2 コマンド出力

フィールド	説明
Destinations	宛先アドレスの数です。
Routes	ルート数です。
Destination	宛先アドレス/マスク長です。
Protocol	ルートを指定したプロトコルです。
SubProtID	ルーティングのサブプロトコルのIDです。
Age	ルーティングテーブルのルートが存在する時間です。
Cost	ルートのコストです。
Preference	ルートの優先順位です。
IpPre	IPプレシーデンスです。
QosLocalID	ローカルQoS IDです。
Tag	ルートタグです。
State	ルート状態です。 • **Active**—アクティブなユニキャストルートです。 • **Adv**—分配できるルートです。 • **Inactive**—非アクティブルートです。 • **NoAdv**—ルータが分配できないルートです。

フィールド	説明
OrigTblID	もとのルーティングテーブルIDです。
OrigVrf	ルートが所属しているもとのVPNインスタンスです。ルートがIPv4パブリックネットワークにある場合、**default-vrf**と表示します。
TableID	ルーティングテーブルのIDです。
OrigAs	もとのAS番号です。
NibID	ネクストホップのIDです。
LastAs	最新のAS番号です。
AttrID	属性IDです。
Neighbor	ルーティングプロトコルによって決定された隣接アドレスです。
Flags	ルートのフラグです。
OrigNextHop	ルートのネクストホップアドレスです。
RealNextHop	ルートの実際のネクストホップです。
BkLabel	バックアップラベルです。
BkNexthop	バックアップネクストホップです。
Interface	ルートに従って転送されるパケットの出力インタフェースです。
BkTunnel ID	バックアップトンネルIDです。
BkInterface	バックアップ出力インタフェースです。
FtnIndex	FTNエントリのインデックスです。
TrafficIndex	トラフィックのインデックスです。範囲は1～64です。 値が不正である場合、**N/A**と表示されます。
Connector	VPN IPv4ルートとともに、BGPピア間で交換されるBGP接続属性です。値はリモートPE装置のIPアドレスです。BGP接続属性はMD VPNで使用されます。BGP接続属性がサポートされていない場合、**N/A**と表示されます。 このフィールドは現在のソフトウェアバージョンでサポートしていません。
Summary Count	ルート数です。

13.1.3 display ip routing-table acl

Syntax

display ip routing-table acl *ipv4-acl-number* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ipv4-acl-number: 標準 ACL を指定します。設定範囲は 2000～2999 です。

verbose: 標準 ACL によって許可されたすべてのルートの詳細情報を表示します。指定しない場合､標準 ACL によって許可されたアクティブルートの概要情報のみ表示します。

説明

display ip routing-table acl コマンドは指定された標準 ACL によって許可されたルートの情報を表示します。

指定された ACL が存在しない、あるいはルールが設定されていない場合、すべてのルートの情報を表示します。

例

標準 ACL 2000 を定義し、ルートのフィルタリングのルールを設定します。

<AP> system-view

[AP] acl basic 2000

[AP-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[AP-acl-ipv4-basic-2000] rule deny source any

標準 ACL 2000 によって許可されたアクティブルートの概要情報を表示します。

[AP-acl-basic-2000] display ip routing-table acl 2000

```
Summary count : 4

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
192.168.1.0/24      Direct 0    0           192.168.1.111   Vlan11
192.168.1.0/32      Direct 0    0           192.168.1.111   Vlan11
192.168.1.111/32    Direct 0    0           127.0.0.1       InLoop0
192.168.1.255/32    Direct 0    0           192.168.1.111   Vlan11
```

コマンド出力は表 1-1 を参照してください。

標準 ACL 2000 によって許可されたすべてのルートの詳細情報を表示します。

<AP> display ip routing-table acl 2000 verbose

```
Summary count : 4

Destination: 192.168.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                 Age: 04h20m37s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000003        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x10080       OrigNextHop: 192.168.1.111
      Label: NULL         RealNextHop: 192.168.1.111
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A

Destination: 192.168.1.0/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000003        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.1.111
      Label: NULL         RealNextHop: 192.168.1.111
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
```

```
  Connector: N/A

Destination: 192.168.1.111/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                 Age: 04h20m37s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000000        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x10004       OrigNextHop: 127.0.0.1
      Label: NULL         RealNextHop: 127.0.0.1
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: InLoopBack0
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A

Destination: 192.168.1.255/32
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x0                 Age: 04h20m37s
       Cost: 0             Preference: 0
      IpPre: N/A           QosLocalID: N/A
        Tag: 0                 State: Active NoAdv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
      NibID: 0x10000003        LastAs: 0
     AttrID: 0xffffffff       Neighbor: 0.0.0.0
      Flags: 0x1008c       OrigNextHop: 192.168.1.111
      Label: NULL         RealNextHop: 192.168.1.111
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A
```

コマンド出力は表 1-2 を参照してください。

13.1.4 display ip routing-table ip-address

Syntax

display ip routing-table *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *ip-address1* **to** *ip-address2* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

ip-address: 宛先 IP アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: マスク長を指定します。設定範囲は 0～32 です。

mask: IP アドレスマスクを指定します。ドットで区切り、10 進数で指定します。

longer-match: マスク長が最長のルートエントリを表示します。

ip-address1 **to** *ip-address2*: 宛先 IP アドレス範囲を指定します。

verbose: アクティブと非アクティブルートを含むルーティングテーブルの詳細情報を表示します。指定しない場合、アクティブルートの概要情報のみ表示します。

説明

display ip routing-table *ip-address* コマンドは指定した宛先アドレスのルート情報を表示します。

display ip routing-table *ip-address1* **to** *ip-address2* コマンドは宛先アドレス範囲のルート情報を表示します。

異なるパラメータを使用してコマンドを実行すると、異なる出力が得られます。

- **display ip routing-table** *ip-address*
  - システムは、入力された宛先 IP アドレスと各アクティブルートエントリのサブネットマスクの AND 演算を行います。
  - 各アクティブルートエントリの宛先 IP アドレスと対応するサブネットマスクの AND 演算を行います。

1 つのエントリに対する 2 つの演算結果が同じである場合、エントリが表示されます。

- **display ip routing-table** *ip-address mask*
  - システムは、入力された宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。
  - 各アクティブルートエントリの宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。

1 つのエントリに対する 2 つの演算結果が同じで､サブネットマスクが入力されたサブネットマスク以下の場合、このエントリが表示されます。

- **display ip routing-table** *ip-address* **longer-match**
  - □ システムは、入力された宛先 IP アドレスと各アクティブルートエントリのサブネットマスクの AND 演算を行います。
  - □ システムは、各アクティブルートエントリの宛先 IP アドレスと対応するサブネットマスクの AND 演算を行います。

複数のエントリに対する 2 つの演算結果が同じ場合、最もマスク長の長いエントリが表示されます。

- **display ip routing-table** *ip-address mask* **longer-match**
  - □ システムは、入力された宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。
  - □ 各アクティブルートエントリの 宛先 IP アドレスと入力されたサブネットマスクの AND 演算を行います。

入力されたサブネットマスク以下のマスクを持つ複数のエントリに対する 2 つの演算結果が同じ場合、マスク長が最長のエントリが表示されます。

- **display ip routing-table** *ip-address1* **to** *ip-address2*

指定した範囲 *ip-address1*/32～*ip-address2*/32 の宛先アドレスのアクティブルートエントリを表示します。

例

宛先 IP アドレス 11.0.0.1 のルートエントリの概要情報を表示します。

<AP> display ip routing-table 11.0.0.1

```
Summary count : 3

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/8          Static 60   0           0.0.0.0         NULL0
11.0.0.0/16         Static 60   0           0.0.0.0         NULL0
11.0.0.0/24         Static 60   0           0.0.0.0         NULL0
```

宛先 IP アドレス 11.0.0.1 およびマスク長 20 のルートの概要情報を表示します。

<AP> display ip routing-table 11.0.0.1 20

```
Summary count : 2

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/8          Static 60   0           0.0.0.0         NULL0
11.0.0.0/16         Static 60   0           0.0.0.0         NULL0
```

宛先アドレス 11.0.0.1 のマスク長が最長のルートの概要情報を表示します。

<AP> display ip routing-table 11.0.0.1 longer-match

```
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/24         Static 60   0           0.0.0.0         NULL0
```

宛先アドレス 11.0.0.1、マスク長 20、マスク長が最長のルートの概要情報を表示します。

<AP> display ip routing-table 11.0.0.1 20 longer-match

```
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
11.0.0.0/16         Static 60   0           0.0.0.0         NULL0
```

宛先アドレス範囲 1.1.1.0～5.5.5.0 の宛先アドレスのルートの概要情報を表示します。

<AP> display ip routing-table 1.1.1.0 to 5.5.5.0

```
Summary count : 4

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.1.1.1/32          Direct 0    0           127.0.0.1       InLoop0
2.2.2.0/24          Direct 0    0           2.2.2.1         Vlan2
3.3.3.1/32          Direct 0    0           127.0.0.1       InLoop0
4.4.4.1/32          Direct 0    0           127.0.0.1       InLoop0
```

13.1.5 display ip routing-table prefix-list

Syntax

display ip routing-table prefix-list *prefix-list-name* [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

prefix-list-name: IP プレフィックスリストを指定します。設定範囲は 1～63 です。大文字、小文字を区別します。

verbose: IP プレフィックスリストによって許可されたすべてのルートの詳細情報を表示します。指定しない場合、IP プレフィックスリストによって許可されたアクティブルートの概要情報を表示します。

説明

display ip routing-table prefix-list コマンドはプレフィックスリストによって許可されたルートの情報を表示します。

指定した IP プレフィックスリストが存在しない場合、すべてのルートの情報を表示します。

例

ルート 1.1.1.0/24 を許可するプレフィックスリスト test を作成します。

<AP> system-view

[AP] ip prefix-list test permit 1.1.1.0 24

IP プレフィックスリストによって許可されたアクティブルートの概要情報を表示します。

[AP] display ip routing-table prefix-list test

```
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.1.1.0/24          Direct 0    0           1.1.1.2         Vlan11
```

コマンド出力は表 1-1 を参照してください。

IP プレフィックスリストによって許可されたすべてのルートの詳細情報を表示します。

[AP] display ip routing-table prefix-list test verbose

```
Summary count : 1

Destination: 1.1.1.0/24
   Protocol: Direct
 Process ID: 0
  SubProtID: 0x1                 Age: 04h20m37s
      Cost: 0             Preference: 0
     IpPre: N/A           QosLocalID: N/A
       Tag: 0                State: Active Adv
  OrigTblID: 0x0             OrigVrf: default-vrf
    TableID: 0x2              OrigAs: 0
     NibID: 0x10000003         LastAs: 0
    AttrID: 0xffffffff       Neighbor: 0.0.0.0
     Flags: 0x1008c       OrigNextHop: 1.1.1.2
     Label: NULL          RealNextHop: 1.1.1.2
```

```
    BkLabel: NULL           BkNextHop: N/A
  Tunnel ID: Invalid         Interface: Vlan-interface11
BkTunnel ID: Invalid       BkInterface: N/A
   FtnIndex: 0x0         TrafficIndex: N/A
  Connector: N/A
```

コマンド出力は表 1-2 を参照してください。

13.1.6 display ip routing-table protocol

Syntax

display ip routing-table protocol *protocol* [**inactive** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

protocol: ルーティングプロトコルを指定します。

inactive: 非アクティブルートの情報を表示します。指定しない場合、アクティブルートと非アクティブルートの情報を表示します。

verbose: ルーティングテーブルの詳細情報を表示します。指定しない場合、ルーティングの概要情報を表示します。

説明

display ip routing-table protocol コマンドはプロトコルによって指定されたルートの情報を表示します。

例

ダイレクトルートの概要情報を表示します。

<AP> display ip routing-table protocol direct

```
Summary count : 9

Direct Routing Table Status : <Active>
Summary count : 9

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
```

```
0.0.0.0/32         Direct 0    0           127.0.0.1       InLoop0
2.2.2.0/24         Direct 0    0           2.2.2.1         Vlan2
2.2.2.0/32         Direct 0    0           2.2.2.1         Vlan2
2.2.2.2/32         Direct 0    0           127.0.0.1       InLoop0
2.2.2.255/32       Direct 0    0           2.2.2.1         Vlan2
127.0.0.0/8        Direct 0    0           127.0.0.1       InLoop0
127.0.0.0/32       Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32       Direct 0    0           127.0.0.1       InLoop0
127.255.255.255/32  Direct 0    0           127.0.0.1       InLoop0

Direct Routing Table Status : <Inactive>
Summary count : 0
```

スタティックルートの概要情報を表示します。

<AP> display ip routing-table protocol static

```
Summary count : 1

Static Routing Table Status : <Active>
Summary count : 0

Static Routing Table Status : <Inactive>
Summary count : 1

Destination/Mask    Proto  Pre  Cost        NextHop         Interface
1.2.3.0/24          Static 60   0           1.2.4.5         Vlan10
```

コマンド出力は表 1-1 を参照してください。

13.1.7 display ip routing-table statistics

Syntax

display ip routing-table statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ip routing-table statistics コマンドは IPv4 ルートの統計情報を表示します。

プロトコルによって指定されたすべてのルート、deleted と記載されたルート、アクティブルート数が含まれます。

例

パブリックネットワークの IPv4 ルートの統計情報を表示します。

<AP> display ip routing-table statistics

```
Total prefixes: 15       Active prefixes: 15

Proto      route      active      added       deleted
DIRECT     12         12          30          18
STATIC      3          3           5           2
RIP         0          0           0           0
OSPF        0          0           0           0
Total      15         15          35          20
```

表 13-3 コマンド出力

フィールド	説明
Proto	ルートを指定したプロトコルです。
route	プロトコルによって指定されたルート数です。
active	アクティブルート数です。
added	ルータが起動あるいはルーティングテーブルが最後に削除した後にルーティングテーブルに追加されたルート数です。
deleted	deletedと記載されたルート数です。一定期間後に削除されます。
Total	ルートの総数です。

13.1.8 ip route-static

Syntax

ip route-static *dest-address* { *mask-length* | *mask* } *interface-type interface-number* [preference *preference*]

ip route-static *dest-address* { *mask-length* | *mask* } *next-hop-address* [preference *preference*]

undo ip route-static *dest-address* { *mask-length* | *mask* } [*interface-type interface-number* | *next-hop-address*] [preference *preference*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

dest-address: スタティックルートの宛先アドレスを指定します。ドットで区切り、10 進数で指定します。

mask-length: IP アドレスのマスク長を指定します。設定範囲は 0〜32 です。

mask: IP アドレスのマスクを指定します。ドットで区切り、10 進数で指定します。

interface-type interface-number: 出力インタフェースのタイプと番号を指定します。詳細はオペレーションマニュアルのセクション 4 *ネットワーク“スタティックルーティング”* を参照してください。

next-hop-address: next hop の IP アドレスをドット付き 10 進表記で指定します。

preference *preference*: スタティックルートの優先順位を指定します。設定範囲は 1〜255 です。デフォルトは 60 です。

説明

ip route-static コマンドはスタティックルートを設定します。

undo ip route-static コマンドは、スタティック ルートを削除します。

宛先 IP アドレスとマスクが両方とも 0.0.0.0 (または 0) の場合、設定されたルートはデフォルト ルートです。デフォルト ルートは、ルーティング テーブルのエントリに一致しないパケットを転送するために使用されます。さまざまなルーティング ポリシーを実装して、さまざまなルート優先度を設定します。たとえば、同じ宛先への複数のルートの負荷分散を有効にするには、ルートに同じ優先順位を割り当てます。ルートが相互にバックアップできるようにするには、ルートに異なる優先度を割り当てます。

例

宛先アドレスが 1.1.1.1/24、ネクストホップ アドレスが 2.2.2.2 のスタティック ルートを設定します。

<AP> system-view

[AP] ip route-static 1.1.1.1 24 2.2.2.2

13.1.9 ip route-static default-preference

Syntax

ip route-static default-preference *default-preference-value*

undo ip route-static default-preference

デフォルト

60

View

System view

定義済みユーザロール

network-admin

パラメータ

default-preference-value: スタティックルートのデフォルトの優先順位を設定します。設定範囲は 1～255 です。

説明

ip route-static default-preference コマンドはスタティックルートのデフォルトの優先順位を設定します。

undo ip route-static default-preference コマンドはデフォルトに戻します。

スタティックルートの優先順位を指定しない場合、デフォルトの優先順位が適用されます。

デフォルトの優先順位を再設定した場合、新しく追加されたスタティックルートが適用されます。

例

スタティックルートのデフォルトの優先順位を 120 に設定します。

<AP> system-view

[AP] ip route-static default-preference 120

13.1.10 reset ip routing-table statistics protocol

Syntax

reset ip routing-table statistics protocol { *protocol* | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

protocol: ルーティングプロトコルのルートの統計情報を削除します。

all: すべての IPv4 ルーティングプロトコルのルートの統計情報を削除します。

説明

reset ip routing-table statistics protocol コマンドは IPv4 ルートの統計情報を削除します。

例

パブリックネットワークのすべての IPv4 ルートの統計情報を削除します。

<AP> reset ip routing-table statistics protocol all

QX-W610 アクセスポイント

コマンドマニュアル

05.AP 管理

本マニュアルは以下に示す章で構成されています。

01-AP 管理

目次

このセクションのページは **5-x-x** です。

1 章 AP 管理 1-1
1.1 AP 管理設定コマンド 1-1
1.1.1 radar-channel-switchback 1-1
1.1.2 region-code 1-2
1.1.3 region-code-lock 1-3
1.1.4 wlan global-configuration 1-4
1.1.5 wlan led-mode 1-4

1章 AP 管理

1.1 AP管理設定コマンド

1.1.1 radar-channel-switchback

Syntax

radar-channel-switchback disable

undo radar-channel-switchback

デフォルト

有効 (undo radar-channel-switchback)

View

Global configuration view

定義済みユーザロール

network-admin

説明

radar-channel-switchback disable コマンドはチャネル復帰機能を OFF に指定します。

undo radar-channel-switchback disable コマンドはデフォルト(チャネル復帰機能を ON) に戻します。

レーダー検出が有効な場合、AP（アクセスポイント）は、現在のチャネルでレーダー信号を検出すると、干渉を避けるためにラジオチャネルを切り替えるか、何もしない状態を保持します。チャネルを切り替えた 30 分後、AP は元のチャネルに戻って動作を再開します。ただし、元のチャネルでレーダー信号が検出され続ける場合、AP は再びラジオチャネルを切り替えるか、何もしない状態を保持し続けます。この機能を使用すると、AP が元のチャネルに戻ることを無効にすることができます。この場合、AP は新しいチャネルを使用し続けます。

メモ：

このコマンドは QX-W610 v7.5.114 を含む以降のバージョンからサポートしています。

例

radar channel switchback 機能を無効にします。

<QX-W610> system-view

[QX-W610] wlan global-configuration

[QX-W610-wlan-global-configuration] radar-channel-switchback disable

1.1.2 region-code

Syntax

region-code *code*

undo region-code

デフォルト

JP

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

code: 地域コードを指定します。 地域コードの詳細については、表 1-1 を参照してください。

表 1-1 地域コード一覧

国	地域コード
Japan	JP

説明

region-code コマンドは地域コードを指定します。

undo region-code コマンドはデフォルトに戻します。

地域コードは、利用可能な周波数、利用可能なチャネル、および送信電力レベルなどの特性を決定します。QX-W610 は日本国内のみでの運用をサポートしています。地域コードの設定をする必要はありません。

例

地域コードを JP に設定します。

<AP> system-view

[AP] wlan global-configuration

[AP-wlan-global-configuration] region-code JP

関連コマンド

region-code-lock

1.1.3 region-code-lock

Syntax

region-code-lock { **disable** | **enable** }

undo region-code-lock

デフォルト

any

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

disable: 地域コードのロックを無効にします。

enable: 地域コードのロックを有効にします。

説明

region-code-lock enable コマンドは地域コードのロックを有効にします。

region-code-lock disable コマンドは地域コードのロックを無効にします。

undo region-code-lock コマンドはデフォルトに戻します。

ロックされると地域コードは変更できません。

例

グローバル地域コードをロックします。

<AP> system-view

[AP] wlan global-configuration

[AP-wlan-global-configuration] region-code-lock enable

関連コマンド

region-code

1.1.4 wlan global-configuration

Syntax

wlan global-configuration

View

System view

定義済みユーザロール

network-admin

説明

wlan global-configuration コマンドを使用して、Global configuration view に遷移します

例

Global configuration view に遷移します。

<AP> system-view

[AP] wlan global-configuration

[AP-wlan-global-configuration]

1.1.5 wlan led-mode

Syntax

wlan led-mode { **always-on** | **awake** | **customer** | **normal** | **quiet** }

undo wlan led-mode

デフォルト

normal

View

System view

定義済みユーザロール

network-admin

パラメータ

always-on： LED が常に緑点灯するモードです。

awake： LED が 1 秒緑点灯、60 秒間消灯を繰り返すモードです。

customer： カスタムされた LED モードです。

normal： 通常モードです。

quiet: LED が常に消灯するモードです。

説明

wlan led-mode コマンドは LED 点灯・点滅パターンを設定します。

undo wlan led-mode コマンドはデフォルトの状態に戻します。デフォルトは normal です。

通常運用中と、locator-blink を使用したときの LED の点灯・点滅パターンは表 1-2 と表 1-3 のとおりです。

表 1-2 運用中の LED の点灯・点滅パターン

状態	normal モード	customer モード
電源が入っていません。	消灯	消灯
装置の起動中に異常が発生しました。	橙点灯	橙点灯
起動しました。有線が未接続です。	橙点滅 (0.5 sec)	橙点滅 (0.5 sec)
装置起動しました。無線端末が未接続です。	緑点灯	橙点滅 (1sec)
5GHz 無線にのみ､端末が接続されています。	青点滅	緑点灯
2.4GHz 無線にのみ、端末が接続されています。	緑点滅 (遅点滅)	青点灯
2.4GHz 無線、5GHz 無線に端末が接続されています。	青・緑交互点滅	青・緑交互点滅
メッシュリンクがdownしています。	橙点滅 (0.5 sec)	橙点滅 (0.5 sec)
5GHz無線にのみ、メッシュリンクしています。	青点滅	緑点灯
2.4GHz無線と5GHz無線にメッシュリンクしています。	緑・青点滅 (0.5 sec)	青・緑点滅 (0.5 sec)

表 1-3 Locator-blink を使用したときの LED の点灯・点滅パターン

状態	normal モード	customer モード
電源が入っていません。	消灯	消灯
装置の起動中に異常が発生しました。	橙点灯	橙点灯
装置起動しました。有線が未接続です。	橙点滅 (0.5 sec)	橙点滅 (0.5 sec)
装置起動しました。無線端末が未接続です。	緑点灯	橙点滅 (1sec)

状態	normal モード	customer モード
5GHz 無線にのみ、端末が接続されています。	青点滅	緑点灯
2.4GHz 無線にのみ、端末が接続されています。	緑点滅 (遅点滅)	青点灯
2.4GHz 無線、5GHz 無線に端末が接続されています。	青・緑交互点滅	青・緑交互点滅
メッシュリンクがdownしています。	橙点滅 (0.5 sec)	橙点滅 (0.5 sec)
5GHz無線にのみ、メッシュリンクしています。	青点滅	緑点灯
2.4GHz無線にのみ、メッシュリンクしています。	緑点滅	青点灯
2.4GHz無線と5GHz無線にメッシュリンクしています。	緑・青点滅 (0.5 sec)	青・緑点滅 (0.5 sec)

🕮 **メモ：**

wlan led-mode コマンドで設定できるのは、コンフィグが読み込まれた後の運用中の LED の点灯・点滅パターンです。起動中の LED の点灯・点滅パターンや LED の色についてはインスタレーションマニュアルをご確認下さい。

例

AP の LED 点灯モードを **normal** に設定します。

<AP> system-view

[AP] wlan led-mode normal

AP の LED 点灯モードを **customer** に設定します。

<AP> system-view

[AP] wlan led-mode customer

QX-W610 アクセスポイント

コマンドマニュアル

06.Radio リソース管理

本マニュアルは以下に示す章で構成されています。

01-Radio の管理と設定
02-WLAN 無線リソース管理
03-バンドナビゲーション
04-チャネルスキャン
05-スペクトル管理

目次

このセクションのページは **6-x-x** です。

1 章 Radio の管理と設定 1-1
1.1 Radio の設定管理コマンド 1-1
1.1.1 a-mpdu 1-1
1.1.2 a-msdu 1-2
1.1.3 beacon-interval 1-3
1.1.4 bss-color 1-4
1.1.5 channel 1-5
1.1.6 channel band-width 1-6
1.1.7 channel-usage measure 1-8
1.1.8 client dot11ac-only 1-9
1.1.9 client dot11ax-only 1-10
1.1.10 client dot11b-forbidden 1-11
1.1.11 client dot11n-only 1-12
1.1.12 client max-count 1-13
1.1.13 continuous-mode 1-14
1.1.14 distance 1-15
1.1.15 dl-ofdma 1-16
1.1.16 dot11ac mandatory maximum-nss 1-17
1.1.17 dot11ac multicast-nss 1-18
1.1.18 dot11ac support maximum-nss 1-19
1.1.19 dot11ax mandatory maximum-nss 1-20
1.1.20 dot11ax multicast-nss 1-21
1.1.21 dot11ax support maximum-nss 1-22
1.1.22 dot11n mandatory maximum-mcs 1-23
1.1.23 dot11n multicast-mcs 1-24
1.1.24 dot11n support maximum-mcs 1-25
1.1.25 dtim 1-26
1.1.26 green-energy-management 1-27
1.1.27 ldpc 1-28
1.1.28 max-power 1-29
1.1.29 mimo 1-31
1.1.30 mu-txbf 1-32
1.1.31 protection-mode 1-34
1.1.32 rate 1-35
1.1.33 short-gi 1-37
1.1.34 shutdown (Radio interface view) 1-38

1.1.35 stbc 1-39
1.1.36 su-txbf 1-40
1.1.37 twt negotiate 1-41
1.1.38 type 1-42
1.1.39 ul-ofdma 1-43
1.1.40 wlan global-configuration 1-44

1章 Radio の管理と設定

1.1 Radioの設定管理コマンド

1.1.1 a-mpdu

Syntax

a-mpdu { **disable** | **enable** }

undo a-mpdu

デフォルト

有効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: A-MPDU アグリゲーション手法を無効にします。

enable: A-MPDU アグリゲーション手法を有効にします。

説明

a-mpdu enable コマンドは A-MPDU アグリゲーション手法を有効にします。

a-mpdu disable コマンドは A-MPDU アグリゲーション手法を無効にします。

undo a-mpdu コマンドはデフォルトに戻します。本コマンドは 802.11n、802.11ac、802.11ax、802.11gac、802.11gax でのみ有効です。

無線モードを 802.11a、802.11b、802.11g に変更すると、本コマンドは無効になります。

例

A-MPDU アグリゲーション手法を無効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] type dot11an

[AP-WLAN-Radio1/0/1] a-mpdu disable

1.1.2 a-msdu

Syntax

a-msdu { **disable** | **enable** }

undo a-msdu

デフォルト

有効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: A-MSDU アグリゲーション手法を無効にします。

enable: A-MSDU アグリゲーション手法を有効にします。

説明

a-msdu enable コマンドは A-MSDU アグリゲーション手法を有効にします。

a-msdu disable コマンドは A-MSDU アグリゲーション手法を無効にします。

undo a-msdu コマンドはデフォルトに戻します。

本コマンドは 802.11n、802.11ac、802.11ax、802.11gac、802.11gax でのみ有効です。

無線モードを 802.11a、802.11b、802.11g に変更すると、本コマンドは無効になります。

装置は A-MSDU の受信はできますが、送信はできません。

例

A-MSDU アグリゲーション手法を無効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] type dot11an

[AP-WLAN-Radio1/0/1] a-msdu disable

1.1.3 beacon-interval

Syntax

beacon-interval *interval*

undo beacon-interval

デフォルト

100TU(Time Unit)

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

interval: ビーコン間隔を 32TU から 8191TU の範囲で指定します。

説明

beacon-interval コマンドはビーコン間隔を設定します。

undo beacon-interval コマンドはデフォルトに戻します。

例

ビーコン間隔を 1000TU に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] beacon-interval 1000

1.1.4 bss-color

Syntax

bss-color { **disable** | **enable** }

undo bss-color

デフォルト

ソフトウェアバージョン 7.5.98 では無効です。コンフィグ上では非表示です。

ソフトウェアバージョン 7.5.105 を含む以降のソフトウェアでは有効です。コンフィグ上では非表示です。

View

Radio interface view

定義済みユーザロール

network-admin

説明

bss-color enable コマンドは BSS カラーリングを有効にします。

bss-color disable コマンドは BSS カラーリングを無効にします。

undo bss-color コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。

BSS カラーリングを使用すると、システムは各 BSS にカラーを割り当て、クライアントへのデータパケットにカラー ID を含めることができます。データパケットにカラー ID が含まれることで、クライアントは関連付いた AP からパケットが送信されたかどうかを識別できます。衝突を避けるために、関連付けられた BSS と同じカラーの 802.11 ax データパケットを検出したクライアントは送信を延期します。 高密度環境で BSS カラーリングを有効にすると、システムパフォーマンスとチャネル使用率が向上します。

例

BSS カラーリングを有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] bss-color enable

関連コマンド

type dot11ax

type dot11gax

1.1.5 channel

Syntax

channel { *channel-number* | **auto** }

undo channel

デフォルト

auto

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

channel-number: 数字でチャネルを指定します。この引数の値の範囲は、地域コードおよび無線モードにより異なります。

auto: AP が自動的に無線チャネルを選択します。

説明

channel コマンドは無線の動作チャネルを設定します。

undo channel コマンドはデフォルトに戻します。

レーダー信号が無線の作動チャネル上で検出されると、チャネルが手動で指定されているか自動的に割り当てられているかにかかわらず、AP はそのチャネルを変更し、指定されたチャネルに 30 分後に戻ります。その後、静止タイマーを始動させます。静止時間内にレーダー信号が検出されなければ、AP はそのチャネルの使用を開始します。静止時間内にレーダー信号が検出されると、AP はチャネルを変更します。

例

動作チャネルを 36 に指定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] channel 36

1.1.6 channel band-width

Syntax

channel band-width { **20** | **40** [**auto-switch**] | **80 | 160** }

undo channel band-width

デフォルト

デフォルトの 帯域幅モードは、以下の通り

802.11ax: 80 MHz

802.11gax: 20 MHz

802.11ac: 80 MHz

802.11g: 20 MHz

802.11an: 40 MHz

802.11gn: 20 MHz

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

20: 帯域幅を 20 MHz に設定します。

40: 帯域幅を 40 MHz に設定します。

80: 帯域幅を 80 MHz に設定します。

auto-switch: 無線は 20MHz から 40MHz までの帯域幅モードを切り替えることができます。このパラメータは 802.11gn、802.11gax のみに適用できます。

160: 帯域幅を 160 MHz に設定します。

説明

channel band-width コマンドは帯域幅モードを設定します。

undo channel band-width コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、および 802.11gax 無線にのみ適用されます。無線のモードを変更すると、新しい無線モードに対するこのコマンドのデフォルト設定に戻ります。無線は、隣接チャネルをボンディングして 40/80/160 チャネルを形成できる場合、指定された 40/80/160 MHz 帯域幅を使用します。隣接するチャネルが 40/80/160 チャネルを形成できない場合、無線は指定された帯域幅よりも小さい次の使用可能な帯域幅を使用します。

たとえば、帯域幅モードは 80 MHz に設定されています。

一緒にボンディングできる隣接チャネルが存在する場合、無線は 80 MHz 帯域幅を使用します。80 MHz チャネルにボンディングできる隣接チャネルが存在しないが、40 MHz チャネルにボンディングできる隣接チャネルが 2 つ存在する場合、40 MHz 帯域幅が使用されます。ボンディングできる隣接チャネルが存在しない場合、無線は 20 MHz 帯域幅を使用します。

例

帯域幅モードを 40MHz に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] channel band-width 40

1.1.7 channel-usage measure

Syntax

channel-usage measure

View

Radio interface view

定義済みユーザロール

network-admin

説明

channel-usage measure コマンドはオンデマンドチャネル使用率計測を実行します。

このコマンドにより、AP はサポートされたチャネルをスキャンできるようになり、スキャン後にチャネル使用率を表示できます。チャネルのスキャンには約 1 秒かかります。

例

無線インタフェース WLAN-Radio 1/0/2 を設定し、オンデマンドチャネル使用率計測を実行します。

<AP> system-view

[AP] interface WLAN-Radio 1/0/2

[AP-WLAN-Radio1/0/2] channel-usage measure

```
Please wait..............Done.
Channel  Usage
1        23%
2        34%
3        26%
4        36%
5        42%
6        39%
7        27%
8        45%
9        29%
10       38%
11       46%
12       30%
13       33%
```

1.1.8 client dot11ac-only

Syntax

client dot11ac-only { **disable** | **enable** }

undo client dot11ac-only

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11ac クライアント限定アクセスを無効にします。

enable: 802.11ac クライアント限定アクセスを有効にします。

説明

client dot11ac-only enable を使用して、クライアント dot11ac-only 機能を有効にします。

client dot11ac-only disable を使用して、クライアント dot11ac-only 機能を無効にします。

undo client dot11ac-only を使用して、デフォルトに戻します。

このコマンドは、802.11ac、802.11ax、および 802.11gax 無線にのみ適用されます。

無線モードを変更すると、コマンドが無効になります。無線にこのコマンドを設定すると、無線は 802.11ac および 802.11ax クライアントのみを受け入れ、無線に関連付けられている非 802.11ac および非 802.11ax クライアントはすべてログオフされます。

例

client dot11ac-only 機能を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1/0/1] client dot11ac-only enable

関連コマンド

dot11ac mandatory maximum-nss

1.1.9 client dot11ax-only

Syntax

client dot11ax-only { **disable** | **enable** }

undo client dot11ax-only

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11ax クライアント限定アクセスを無効にします。

enable: 802.11ax クライアント限定アクセスを有効にします。

説明

client dot11ax-only enable を使用して、クライアント dot11ax-only 機能を有効にします。

client dot11ax-only disable を使用して、クライアント dot11ax-only 機能を無効にします。

undo client dot11ax-only を使用して、デフォルトに戻します。

このコマンドは、802.11ax および 802.11gax 無線にのみ適用されます。無線モードを変更すると、コマンドが無効になります。無線にこのコマンドを設定すると、無線は 802.11ax クライアントのみを受け入れ、無線に関連付けられているすべての非 802.11ax クライアントはログオフされます。

例

client dot11ac-only 機能を有効にします。

ap ap1 の Enable the client dot11ax-only 機能を有効にします。

<AP> system-view

[AP] wlan ap ap1 model W610

[AP-wlan-ap-ap1] radio 1

[AP-wlan-ap-ap1-radio-1] type dot11ax

[AP-wlan-ap-ap1-radio-1] client dot11ax-only enable

ap group 1 の client dot11ax-only 機能を有効にします。

<AP> system-view

[AP] wlan ap-group 1

[AP-wlan-ap-group-1] ap-model W610

[AP-wlan-ap-group-1-ap-model-W610] radio 1

[AP-wlan-ap-group-1-ap-model-W610-radio-1] client dot11ax-only enable

client dot11ax-only 機能を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1/0/1] client dot11ax-only enable

関連コマンド

dot11ax mandatory maximum-nss

1.1.10 client dot11b-forbidden

Syntax

client dot11b-forbidden { **disable** | **enable** }

undo client dot11b-forbidden

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11b クライアント拒否を有効にします。

enable: 802.11b クライアント拒否を無効にします。

説明

client dot11b-forbidden enable コマンドは 802.11b クライアントの接続を拒否します。

client dot11b-forbidden disable コマンドは 802.11b クライアント拒否を無効にします。

undo client dot11b-forbidden コマンドデフォルトに戻します。

802.11g、802.11gn 無線で 802.11b クライアントを拒否することにより、低速な 802.11b クライアントの影響を減少させ、無線データ転送を高速化することができます。

例

WLAN-radio 1/0/2 で、802.11b クライアントを拒否します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-wlan-radio-1/0/2] client dot11b-forbidden enable

1.1.11 client dot11n-only

Syntax

client dot11n-only { **disable** | **enable** }

undo client dot11n-only

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: 802.11n/ac/ax クライアント限定アクセスを無効にします。

enable: 802.11n/ac/ax クライアント限定アクセスを有効にします。

説明

client dot11n-only enable コマンドは 802.11ac 無線で 802.11an/ac クライアントの接続のみを許可し、802.11ax 無線で 802.11an/ac/ax クライアントの接続のみを許可します。

client dot11n-only disable コマンドは 802.11n/ac/ax クライアント限定アクセスを無効にします。

undo client dot11n-only コマンドはデフォルトに戻します。

本コマンドは 802.11n、802.11ac、802.11ax 無線にのみ適用可能です。無線モードを 802.11a/b/g に変更することで、本機能は無効になります。

本コマンドを有効にすると、802.11a/b/g クライアントはログオフされます。

例

802.11n/ac/ax クライアント限定アクセスを有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] client dot11n-only enable

1.1.12 client max-count

Syntax

client max-count *max-number*

undo client max-count

デフォルト

制限なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

max-number: AP に接続できるクライアントの最大数を指定します。範囲は 1～128 です。

説明

client max-count コマンドは AP に接続できるクライアントの最大数を設定します。

undo client max-count コマンドはデフォルトに戻します。

クライアント数が最大に達すると、AP は新しいクライアントの許可を停止します。

例

AP に接続できるクライアントの最大数を 38 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] client max-count 38

1.1.13 continuous-mode

Syntax

continuous-mode { **mcs** *mcs-index* | **nss** *nss-index* **vht-mcs** *vhtmcs-index* | **rate** *rate-value* }

undo continuous-mode

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

mcs *mcs-index*: MCS インデックスを 0～76 の範囲で指定します。このオプションは 802.11n、802.11ac、802.11gac 無線にのみ適用します。

nss *nss-index* **vht-mcs** *vhtmcs-index*: VHT-MCS インデックスを指定します。*nss-index* の設定範囲は 1～8、*vhtmcs-index* の設定範囲は 0～9 です。このオプションは 802.11ac、802.11gac 無線にのみ適用します。

rate *rate-value*: 送信レートを Mbps で指定します。このオプションはすべての無線タイプに適用します。

説明

continuous-mode コマンドは連続モードを有効にします。

undo continuous-mode コマンドはデフォルトに戻します。

この機能はネットワークテストにのみ使用されます。それ以外の環境では使用しないでください。

指定されたレートで連続データパケット送信を可能にします。この機能が有効になっているときは、送信レートを変更する以外の操作は実行しないでください。

例

連続モードを有効にし、伝送速度を 6Mbps に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] continuous-mode rate 6

1.1.14 distance

Syntax

distance *distance*

undo distance

デフォルト

1km

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

distance: 最大伝送距離を指定します。範囲は 1～40km です。

説明

distance コマンドは最大伝送距離を設定します。

undo distance コマンドはデフォルトに戻します。

例

最大伝送距離を 5km に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] distance 5

1.1.15 dl-ofdma

Syntax

dl-ofdma { **disable** | **enable** }

undo dl-ofdma

デフォルト

ソフトウェアバージョン 7.5.98 では無効です。コンフィグ上では非表示です。

ソフトウェアバージョン 7.5.105 を含む以降のソフトウェアでは有効です。コンフィグ上では非表示です。

View

Radio interface view

定義済みユーザロール

network-admin

説明

dl-ofdma enable コマンドはダウンリンク OFDMA を有効にします。

dl-ofdma disable コマンドはダウンリンク OFDMA を無効にします。

undo dl-ofdma コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。 OFDMA は、小さなデータパケットが送信される高密度環境で有効にすると、次の利点があります

- 複数ユーザへの同時通信
- 無線使用率の向上
- 転送遅延の短縮
- 衝突バックオフの削減

例

ダウンリンク OFDMA を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/2] dl-ofdma enable

1.1.16 dot11ac mandatory maximum-nss

Syntax

dot11ac mandatory maximum-nss *nss-number*

undo dot11ac mandatory maximum-nss

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大必須 NSS を指定します。範囲は 1～8 です。

説明

dot11ac mandatory maximum-nss コマンドは最大必須 NSS を設定します。

undo dot11ac mandatory maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ac、802.11gac 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドは無効になります。

最大必須 NSS は、最大サポート NSS より大きくすることはできません。

最大必須 NSS の変更後、無線に接続している、変更された NSS をサポートしないクライアントの接続が解除されます。

例

最大必須 NSS を 7 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1/0/1] dot11ac mandatory maximum-nss 7

関連コマンド

dot11ac support maximum-nss

1.1.17 dot11ac multicast-nss

Syntax

dot11ac multicast-nss *nss-number* **vht-mcs** *index*

undo dot11ac multicast-nss

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

nss-number: マルチキャスト NSS を指定します。範囲は 1〜8 です。

index: VHT-MCS インデックスを指定します。範囲は 0〜9 です。

説明

dot11ac multicast-nss コマンドはマルチキャスト NSS と VHT-MCS インデックスを設定します。

undo dot11ac multicast-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ac、802.11gac 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドは無効になります。

本コマンドを設定する前に、**dot11ac mandatory maximum-nss** コマンドを設定しなければいけません。

マルチキャスト NSS は、最大必須 NSS より大きくすることはできません。

例

最大必須 MSS を 2 に、マルチキャスト NSS を 2 に、VHT-MCS インデックスを 2 にそれぞれ設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1/0/1] dot11ac mandatory maximum-nss 2

[AP-wlan-radio-1/0/1] dot11ac multicast-nss 2 vht-mcs 2

関連コマンド

dot11ac mandatory maximum-nss

1.1.18 dot11ac support maximum-nss

Syntax

dot11ac support maximum-nss *nss-number*

undo dot11ac support maximum-nss

デフォルト

8

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大サポート NSS を指定します。範囲は 1～8 です。

説明

dot11ac support maximum-nss コマンドは最大サポート NSS を設定します。

undo dot11ac support maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ac、802.11gac 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドは無効になります。

最大サポート NSS は、最大必須 NSS より小さくすることはできません。

例

最大サポート NSS を 7 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1/0/1] dot11ac support maximum-nss 7

関連コマンド

dot11ac mandatory maximum-nss

1.1.19 dot11ax mandatory maximum-nss

Syntax

dot11ax mandatory maximum-nss *nss-number*

undo dot11ax mandatory maximum-nss

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大必須 NSS を指定します。範囲は 1～8 です。

説明

dot11ax mandatory maximum-nss コマンドは最大必須 NSS を設定します。

undo dot11ax mandatory maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ax、802.11gax 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドは無効になります。

最大必須 NSS は、最大サポート NSS より大きくすることはできません。

最大必須 NSS の変更後、無線に接続している、変更された NSS をサポートしないクライアントの接続が解除されます。

関連コマンド

dot11ax support maximum-nss

1.1.20 dot11ax multicast-nss

Syntax

dot11ax multicast-nss *nss-number* **he-mcs** *index*

undo dot11ax multicast-nss

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

nss-number: マルチキャスト NSS を指定します。範囲は 1〜8 です。

index: he-mcs インデックスを指定します。範囲は 0〜11 です。

説明

dot11ax multicast-nss コマンドはマルチキャスト NSS と he-mcs インデックスを設定します。

undo dot11ax multicast-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ax、802.11gax 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドは無効になります。

本コマンドを設定する前に、**dot11ax mandatory maximum-nss** コマンドを設定しなければいけません。

マルチキャスト NSS は、最大必須 NSS より大きくすることはできません。

関連コマンド

dot11ax mandatory maximum-nss

1.1.21 dot11ax support maximum-nss

Syntax

dot11ax support maximum-nss *nss-number*

undo dot11ax support maximum-nss

デフォルト

8

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

nss-number: 最大サポート NSS を指定します。範囲は 1～8 です。

説明

dot11ax support maximum-nss コマンドは最大サポート NSS を設定します。

undo dot11ax support maximum-nss コマンドはデフォルトに戻します。

本コマンドは、802.11ax、802.11gax 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g、または 802.11n に変更すると、コマンドは無効になります。

最大サポート NSS は、最大必須 NSS より小さくすることはできません。

関連コマンド

dot11ax mandatory maximum-nss

1.1.22 dot11n mandatory maximum-mcs

Syntax

dot11n mandatory maximum-mcs *index*

undo dot11n mandatory maximum-mcs

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

index: 最大必須 MCS インデックスを指定します。範囲は 0～76 です。

説明

dot11n mandatory maximum-mcs コマンドは最大必須 MCS インデックスを設定します。

undo dot11n mandatory maximum-mcs コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、802.11gac 無線にのみ適用されます。無線モードを 802.11a、802.11b、802.11g に変更した場合、コマンドは無効になります。

最大必須 MCS インデックスは、**dot11n multicast-mcs** コマンドを設定する前に設定しなければいけません。

最大必須 MCS インデックスの変更後、無線に接続している、変更された MCS インデックスをサポートしないクライアントの接続が解除されます。

例

最大必須 MCS インデックスを 14 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] dot11n mandatory maximum-mcs 14

1.1.23 dot11n multicast-mcs

Syntax

dot11n multicast-mcs *index*

undo dot11n multicast-mcs

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

index: マルチキャスト MCS インデックスを指定します。範囲は 0〜76 です。

説明

dot11n multicast-mcs コマンドはマルチキャスト MCS インデックスを設定します。

undo dot11n multicast-mcs コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g に変更すると、本コマンドは無効になります。

マルチキャスト MCS インデックスは、無線と 802.11n、802.11ac、802.11ax クライアントが接続されている場合のみ有効になります。

802.11a/b/g クライアントが存在する場合、AP とクライアントは、パケットのマルチキャストにおいて 802.11a/b/g マルチキャストレートを使用します。

マルチキャスト MCS インデックスは、帯域モードが 20MHz か 40MHz かによらず、20MHz 帯域モードのレートにマッピングされます。

例

マルチキャスト MCS インデックスを 14 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] dot11n mandatory maximum-mcs 15

[AP-WLAN-Radio1/0/1] dot11n multicast-mcs 14

1.1.24 dot11n support maximum-mcs

Syntax

dot11n support maximum-mcs *index*

undo dot11n support maximum-mcs

デフォルト

76

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

index: 最大サポート MCS インデックスを指定します。範囲は 0〜76 です。

説明

dot11n support maximum-mcs コマンドは最大サポート MCS インデックスを設定します。

undo dot11n support maximum-mcs コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、802.11gac 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g に変更すると、本コマンドは無効になります。

最大サポート MCS インデックスは、最大必須 MCS インデックスより小さくなることはできません。

例

最大サポート MCS インデックスを 14 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] dot11n support maximum-mcs 14

1.1.25 dtim

Syntax

dtim *counter*

undo dtim

デフォルト

DTIM 間隔は 1 です。AP はバッファリングされたブロードキャストおよびマルチキャストフレームを毎回ビーコンフレームごとに送信します。

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

counter: DTIM 間隔を指定します。範囲は 1～31 です。

説明

dtim コマンドは DTIM（Delivery Traffic Indication Map）間隔を設定します。

undo dtim コマンドはデフォルトに戻します。

AP は、DTIM（Delivery Traffic Indication Map）に従ったビーコンを周期的にブロードキャストします。ビーコンをブロードキャストした後、AP は DTIM 間隔の値に基づいてバッファリングされたブロードキャストおよびマルチキャストフレームを送信します。例えば、DTIM 間隔を 5 に設定した場合、AP はバッファリングされたブロードキャストおよびマルチキャストフレームを 5 ビーコンフレームごとに送信します。

例

DTIM 間隔を 5 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio1/0/1] dtim 5

1.1.26 green-energy-management

Syntax

green-energy-management { **disable** | **enable** }

undo green-energy-management

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: エネルギ節約機能を無効にします。

enable: エネルギ節約機能を有効にします。

説明

green-energy-management enable コマンドはエネルギ節約機能を有効にします。

green-energy-management disable コマンドはエネルギ節約機能を無効にします。

undo green-energy-management コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、802.11gac 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g に変更すると、本コマンドは無効になります。

エネルギ節約機能を有効にした後、無線に接続されたクライアントが存在しない場合、無線の MIMO モードを自動的に 1x1 に変更し、消費電力を削減します。

例

エネルギ節約機能を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] green-energy-management enable

1.1.27 ldpc

Syntax

ldpc { **disable** | **enable** }

undo ldpc

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: LDPC を無効にします。

enable: LDPC を有効にします。

説明

ldpc enable コマンドは LDPC を有効にします。

ldpc disable コマンドは LDPC を無効にします。

undo ldpc コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、802.11gac 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g に変更すると、本コマンドは無効になります。

例

LDPC を無効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1/0/1] ldpc disable

1.1.28 max-power

Syntax

max-power *radio-power*

undo max-power

デフォルト

サポートしている最大伝送電力値が指定されています。

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

radio-power : 最大伝送電力を指定します。

QX-W610 Radio 1/0/1 の設定可能範囲は、

W52 、W53 帯を使用していて、かつ、帯域幅モードを 20 MHz に設定している場合は、1～16 (dBm)です。

W52 、 W53 帯を使用していて、かつ、帯域幅モードを 40 MHz、80 MHz、160 MHz に設定している場合は、1～15 (dBm)です。

W56 帯を使用している場合は、1～21 (dBm)です。

QX-W610 Radio 1/0/2 の設定可能範囲は、

タイプを 802.11gax や 802.11gn で設定している場合は、1～17 (dBm) です。

タイプを 802.11g で設定している場合は、1～16 (dBm) です。

タイプを 802.11b で設定している場合は、1～13 (dBm) です。

説明

max-power コマンドは最大伝送電力を設定します。

undo max-power コマンドはデフォルトに戻します。

無線でサポートされる伝送電力の範囲は、チャネル、無線モード、アンテナタイプ、帯域幅モードにより変化します。最大伝送電力を設定後に無線に対するこれらの特性を変更した場合、設定された最大伝送電力がサポートされた伝送電力の範囲外になる可能性があります。この場合、システムは自動的に最大伝送電力を有効な値に適応させます。

例

最大伝送電力を 10 dBm に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] max-power 10

1.1.29 mimo

Syntax

mimo { **1x1** | **2x2** }

undo mimo

デフォルト

2x2

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

1x1: 1 つの空間ストリームを通じて信号を送受信します。

2x2: 2 つの空間ストリームを通じて信号を送受信します。

説明

mimo コマンドは、無線の MIMO モードを設定します。

undo mimo コマンドは、デフォルトに戻します。

MIMO により、無線は複数の空間ストリームを介して無線信号を送受信できます。これにより、より高い帯域幅を必要とせずに、システム容量とスペクトル使用率が向上します。

例

MIMO モードを 2x2 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] mimo 2x2

1.1.30 mu-txbf

Syntax

mu-txbf { **disable** | **enable** }

undo mu-txbf

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: マルチユーザ TxBF（transmit beamforming）を無効にします。

enable: マルチユーザ TxBF（transmit beamforming）を有効にします。

説明

mu-txbf enable コマンドはマルチユーザ TxBF（transmit beamforming）を有効にします。

mu-txbf disable コマンドはマルチユーザ TxBF を無効にします。

undo mu-txbf コマンドはデフォルトに戻します。

本コマンドは、802.11ac、802.11gac 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g、802.11n に変更すると、本コマンドは無効になります。

TxBF により、AP はチャネル情報に基づいた伝送パラメータを適応し、意図したクライアントに RF 信号を送信できます。この機能を使用することで RF 信号品質が向上します。

マルチユーザ TxBF は 802.11ac Wave2 の一部です。マルチユーザ TxBF により、AP は接続したクライアントに異なる RF 信号を送信でき、干渉と伝送遅延が低減します。これにより、トラフィックスループットと帯域幅使用率が向上します。マルチユーザ TxBF は、クライアントが多数存在し、高帯域幅使用率と低伝送遅延が要求される WLAN に適用できます。

マルチユーザ TxBF はシングルユーザ TxBF が有効な場合のみ適用されます。

マルチユーザ TxBF が有効にされた AP に対する、デフォルトの MIMO 設定を修正しないことを推奨します。

例

Multi-user TxBF を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] su-txbf enable

[AP-WLAN-Radio1/0/1] mu-txbf enable

関連コマンド

su-txbf

1.1.31 protection-mode

Syntax

protection-mode { **cts-to-self** | **rts-cts** }

undo protection-mode

デフォルト

CTS-to-self

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

cts-to-self ：CTS-to-self モードを指定します。

rts-cts ：RTS/CTS モードを指定します。

説明

protection-mode コマンドは衝突回避モードを設定します。

undo protection-mode コマンドはデフォルト (CTS-to-self) に戻します。

AP に対して以下の衝突回避モードのいずれかを指定することができます。

- RTS/CTS： AP はデータをクライアントに送信する前に RTS パケットをクライアントに送信します。RTS パケットを受信した後、クライアントは CTS パケットを AP に送信します。AP は CTS パケットを受信した後にデータを送信し始めます。RTS または CTS パケットを検出した他のデバイスは、特定の時間内にデータを送信しません。
- CTS-to-self： AP はデータをクライアントに送信する前に、送信先 MAC アドレスとして自分の MAC アドレスを指定した CTS パケットを送信します。CTS-to-self パケットを受信した後、AP はデータの送信を開始し、CTS-to-self パケットを検出した他のデバイスは特定の時間内にデータを送信しません。

例

衝突回避モードとして、RTS/CTS を設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] protection-mode rts-cts

1.1.32 rate

Syntax

rate { **multicast** { **auto** | **rate-value** } | { **disabled** | **mandatory** | **supported** } *rate-value* }

undo rate

デフォルト

- 802.11a/802.11an/802.11ac/802.11ax
  - 禁止速度－なし
  - 必須速度－6、12、24
  - マルチキャスト速度－必須速度から選択されます。
  - サポート速度－9、18、36、48、54
- 802.11b
  - 禁止速度－なし
  - 必須速度－1、2
  - マルチキャスト速度－必須速度から選択されます。
  - サポート速度－5.5、11
- 802.11g/802.11gn/802.11gac
  - 禁止速度－なし
  - 必須速度－1、2、5.5、11
  - マルチキャスト速度－必須速度から選択されます。
  - サポート速度－6、9、12、18、24、36、48、54

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disabled: AP で使用できない速度を指定します。

mandatory: AP と接続するためにクライアントがサポートしなければならない速度を指定します。

multicast: AP がパケットをマルチキャストする速度を指定します。マルチキャスト速度は、必須速度の中から選択されなければなりません。

supported: AP がサポートする速度を指定します。クライアントが AP と接続した後に、クライアントは AP と通信するために、サポートされた速度の中から、より高い速度や低い速度を選択することが可能です。

auto: マルチキャスト速度として、必須速度を自動的に選択します。

rate-value: 速度を Mbps で指定します。スペース区切りで複数の速度を設定することができます。利用可能な引数は以下の通りです。

- **802.11a/802.11an/802.11ac/802.11ax**－6、9、12、18、24、36、48、54
- **802.11b**－1、2、5.5、11
- **802.11g/802.11gn/802.11gac**－1、2、5.5、6、9、11、12、18、24、36、48、54

説明

rate コマンドは無線の伝送速度を設定します。

undo rate コマンドはデフォルトに戻します。

必須速度とマルチキャスト速度を未設定にすることはできません。必須速度が 1 種類しかない場合は、サポート速度または禁止速度として必須速度を指定することはできません。

例

必須速度として 6Mbps、12Mbps、24Mbps を設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] rate mandatory 6 12 24

1.1.33 short-gi

Syntax

short-gi { **disable** | **enable** }

undo short-gi

デフォルト

有効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable： ショート GI を無効にします。

enable： ショート GI を有効にします。

説明

short-gi enable コマンドは Short Guard Interval (GI) を有効にします。

short-gi disable コマンドは Short Guard Interval (GI) を無効にします。

undo short-gi コマンドはデフォルトに戻します。

このコマンドは、ラジオタイプが、802.11n、802.11ac、802.11gac、802.11gax にのみ適用されます。

ラジオタイプを、802.11a、802.11b、802.11g に変更すると、コマンドは無効になります。

例

Short GI を無効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1/0/1] short-gi disable

1.1.34 shutdown (Radio interface view)

Syntax

shutdown

undo shutdown

デフォルト

Radio-interface はデフォルト アップ状態 (undo shutdown) です。

View

Radio interface view

定義済みユーザロール

network-admin

説明

shutdown コマンドは Radio interface をダウン状態にします。

undo shutdown コマンドは Radio interface をアップ状態にします。

例

Radio インタフェース 1 をダウン状態に変更します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1/0/1] shutdown

Radio 1/0/1 のインタフェースのステータスが変更されたログが表示されます。

[AP-wlan-radio-1/0/1] %Dec 9 10:15:55:027 2024 QX-W610 IFNET/3/PHY_UPDOWN: Physical state on the interface WLAN-Radio1/0/1 changed to down.

display interface WLAN-Radio brief コマンドを実行して、Link ステータスが、「ADM」となったことを確認します。

[AP] display interface WLAN-Radio brief

Brief information on interfaces in bridge mode:

Link: ADM - administratively down; Stby - standby

Speed: (a) - auto

Duplex: (a)/A - auto; H - half; F - full

Type: A - access; T - trunk; H - hybrid

Interface	Link Speed	Duplex Type	PVID	Description
WLAN-Radio1/0/1	ADM --	--	--	--
WLAN-Radio1/0/2	UP --	--	--	--

1.1.35 stbc

Syntax

stbc { **disable** | **enable** }

undo stbc

デフォルト

有効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: STBC を無効にします。

enable: STBC を有効にします。

説明

stbc enable コマンドは STBC を有効にします。

stbc disable コマンドは STBC を無効にします。

undo stbc コマンドはデフォルトに戻します。

本コマンドは、802.11n、802.11ac、802.11ax、802.11gac 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g に変更すると、本コマンドは無効になります。

例

STBC を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1/0/1] stbc enable

1.1.36 su-txbf

Syntax

su-txbf { **disable** | **enable** }

undo su-txbf

デフォルト

Single-user TxBF は、無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: シングルユーザ TxBF を無効にします。

enable: シングルユーザ TxBF を有効にします。

説明

su-txbf enable コマンドはシングルユーザ TxBF を有効にします。

su-txbf disable コマンドはシングルユーザ TxBF を無効にします。

undo su-txbf コマンドはデフォルトに戻します。

本コマンドは、802.11ac、802.11gac 無線でのみ適用されます。無線モードを 802.11a、802.11b、802.11g、802.11n に変更すると、本コマンドは無効になります。

シングルユーザ TxBF により、AP は 1 つの意図したクライアントへの信号を向上できます。シングルユーザ TxBF は、クライアントが広範囲に存在し、ネットワーク品質がプアで信号の減衰が著しい WLAN に適用できます。

例

シングルユーザ TxBF を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] su-txbf enable

1.1.37 twt negotiate

Syntax

twt negotiate { **disable** | **enable** }

undo twt negotiate

デフォルト

ソフトウェアバージョン 7.5.105 を含む以降のソフトウェアでは有効です。コンフィグ上では非表示です。

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

なし

説明

twt negotiate enable コマンドは Target Wake Time (TWT) ネゴシエーションを有効にします。

twt negotiate disable コマンドは TWT ネゴシエーションを無効にします。

undo twt negotiate コマンドはデフォルトに戻します。

例

TWT ネゴシエーションを有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] twt negotiate enable

🕮 **メモ：**

- **twt negotiate** コマンドはソフトウェアバージョン 7.5.105 を含む以降のソフトウェアからサポートしています。

1.1.38 type

Syntax

type { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | **dot11gax | dot11gn** }

undo type

デフォルト

Radio1、Radio2 の無線モードは、それぞれ dot11ax、dot11gax です。

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a 無線モードを指定します。

dot11ac: 802.11ac 無線モードを指定します。

dot11an: 802.11n (5 GHz) 無線モードを指定します。

dot11ax: 802.11ax 無線モードを指定します。

dot11b: 802.11b 無線モードを指定します。

dot11g: 802.11g 無線モードを指定します。

dot11gax: 802.11gax 無線モードを指定します。

dot11gn: 802.11n (2.4 GHz) 無線モードを指定します。

説明

type コマンドは無線モードを指定します。

undo type コマンドはデフォルトに戻します。

⚠ **注意:**

有効な無線のモードを変更すると、帰属しているすべてのクライアントが切断されます。

例

無線モードを 802.11n (5 GHz)に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] type dot11an

1.1.39 ul-ofdma

Syntax

ul-ofdma { **disable** | **enable** }

undo ul-ofdma

デフォルト

ソフトウェアバージョン 7.5.98 では無効です。コンフィグ上では非表示です。

ソフトウェアバージョン 7.5.105 を含む以降のソフトウェアでは有効です。コンフィグ上では非表示です。

View

Radio interface view

定義済みユーザロール

network-admin

説明

ul-ofdma enable コマンドはアップリンク OFDMA を有効にします。

ul-ofdma disable コマンドはアップリンク OFDMA を無効にします。

undo ul-ofdma コマンドはデフォルトに戻します。

このコマンドは、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 a/b/g/n/ac/gac に変更すると、設定が削除されます。 OFDMA は、小さなデータパケットが送信される高密度環境で有効にすると、次の利点があります。

- 複数ユーザへの同時通信
- 無線使用率の向上
- 転送遅延の短縮
- 衝突バックオフの削減

例

アップリンク OFDMA を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] ul-ofdma enable

1.1.40 wlan global-configuration

Syntax

wlan global-configuration

View

System view

定義済みユーザロール

network-admin

説明

wlan global-configuration コマンドは global configuration view へ移行します

例

global configuration view へ移行します。

<AP> system-view

[AP] wlan global-configuration

[AP-wlan-global-configuration]

目次

このセクションのページは **6-x-x** です。

2 章 WLAN 無線リソース管理 2-1
2.1 WLAN 無線リソースの計測コマンド 2-1
2.1.1 display wlan measure-report 2-1
2.1.2 measure 2-5
2.1.3 measure-duration 2-7
2.1.4 measure-interval 2-8
2.1.5 resource-measure 2-9
2.1.6 rm-capability mode 2-10

2章 WLAN 無線リソース管理

2.1 WLAN無線リソースの計測コマンド

2.1.1 display wlan measure-report

Syntax

display wlan measure-report interface *interface-type interface-number* [**client mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: 無線インタフェースとタイプと番号を指定します。

client mac-address *mac-address*: クライアントを MAC アドレスで指定します。 このオプションを指定しない場合、すべてのクライアントの計測結果を表示します。

説明

display wlan measure-report コマンドは計測結果を表示します。

例

AP ap1 の無線 2 に接続したクライアントの計測結果を表示します。

<AP> display wlan measure-report interface wlan-radio 1/0/1

```
Total number of clients: 1

Client MAC address                          : 0aef-e760-3587
Link measurement:
  Link margin                              : 2 dBm
  RCPI                                     : -85 dBm
  RSNI                                     : 53 dBm
Noise histogram:
  Antenna ID                               : 3
  ANPI                                     : -56 dBm
```

```
  IPI0 to IPI10 density                    : 5 12 16 13 8 5 5 15 17 1 3
Spectrum measurement:
  Transmit power                          : 20 dBm
  BSS                                    : Detected
  OFDM preamble                           : Detected
  Radar                                  : Detected
  Unidentified signal                      : Undetected
  CCA busy fraction                       : 60
  RPI0 to RPI7 density                     : 3 7 11 19 15 23 15 7
Frame report entry:
  BSSID                                  : a072-2351-e253
  PHY type                               : fhss
  Average RCPI                            : -10 dBm
  Last RSNI                              : 2 dBm
  Last RCPI                              : -20 dBm
  Frames                                 : 1
Dot11BSSAverageAccessDelay group:
  Average access delay                     : 32 ms
  BestEffort average access delay            : 1 ms
  Background average access delay            : 1 ms
  Video average access delay                : 1 ms
  Voice average access delay                : 1 ms
  Clients                                : 32
  Channel utilization rate                   : 11
Transmit stream:
  Traffic ID                             : 0
  Sent MSDUs                             : 60
  Discarded MSDUs                         : 5
  Failed MSDUs                           : 3
  MSDUs resent multiple times               : 3
  Lost QoS CF-Polls                       : 2
  Average queue delay                      : 2 ms
  Average transmit delay                    : 1 ms
  Bin0 range                             : 0 to 10 ms
  Bin0 to Bin5                            : 5 10 10 5 10 10
```

表 2-1 コマンド出力

フィールド	説明
Link margin	受信したRSSIと最低の利用可能なRSSIとの間のギャップ。
RCPI	受信チャネル電力インジケータ。
RSNI	受信信号対雑音インジケータ。
ANPI	測定中の平均雑音電力インジケータ。
IPI0 to IPI10 density	測定期間全体に対する異なるIPI範囲の時間の割合。 IPInはIPI範囲を表します。 nの値は1～10の範囲です。 • 0: IPI <= –92 dBm. • **1:** –92 dBm < IPI <= –89 dBm. • **2:** –89 dBm < IPI <= –86 dBm. • **3:** –86 dBm < IPI <= –83 dBm. • **4:** –83 dBm < IPI <= –80 dBm. • **5:** –80 dBm < IPI <= –75 dBm • **6:** –75 dBm < IPI <= –70 dBm. • **7:** –70 dBm < IPI <= –65 dBm. • **8:** –65 dBm < IPI <= –60 dBm. • **9:** –60 dBm < IPI <= –55 dBm. • **10:** –55 dBm < IPI.
Transmit power	クライアントの送信電力。
BSS	クライアントが他のBSSからの無線パケットを検出したかどうか。
OFDM preamble	クライアントがOFDMプリアンブルを検出したかどうか。
Radar	クライアントがレーダー信号を検出したかどうか。
Unidentified signal	クライアントが未知の信号を検出したかどうか。
CCA busy fraction	全測定期間に対するチャネルのビジー時間の割合。
RPI0 to RPI7 density	測定期間全体に対してRPIが使用される時間の割合。 RPInはRPI範囲を表します。 nの値は1～7の範囲です。 • **0:** RPI <= –87 dBm. • **1:** –87 dBm < RPI <= –82 dBm. • **2:** –82 dBm < RPI <= –77 dBm. • **3:** –77 dBm < RPI <= –72 dBm. • **4:** –72 dBm < RPI <= –67 dBm.

フィールド	説明
	● **5:** –67 dBm < RPI <= –62 dBm. ● **6:** –62 dBm < RPI <= –57 dBm. ● **7:** –57 dBm < RPI.
PHY type	物理メディアの種類 ● fhss. ● dsss. ● irbaseband. ● ofdm. ● hrdsss. ● erp.
Frames	測定中の同じMACアドレスとBSSIDからのフレーム数。
Bin0 range	Bin0の値の範囲。
Bin0 to Bin5	平均遅延範囲ごとに正常に送信されたMSDUの数。 Binxは平均遅延範囲を表します。 xの値は0～5の範囲です。 ● **Bin0**: Delay< 10 ms. ● **Bin1**: 10 ms <= Delay < 20 ms. ● **Bin2**: 20 ms <= Delay < 40 ms. ● **Bin3**: 40 ms <= Delay < 80 ms. ● **Bin4**: 80 ms <= Delay < 160 ms. ● **Bin5**: 160 ms <= Delay.

2.1.2 measure

Syntax

measure { **all** | **link** | **neighbor** | **radio** | **spectrum** | **tpc** } { **disable** | **enable** }

undo measure

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

all: すべての測定機能を指定します。

link: リンク測定を指定します。 リンク測定は、要求されたリンクの RCPI、RSNI、リンク冗長性を測定します。

neighbor: 隣接測定を指定します。 近隣測定は、隣接 AP のチャネルおよび BSSID を測定します。

radio: 無線測定を指定します。 無線測定は、チャネル負荷、雑音ヒストグラム、ビーコン、フレーム、station 統計、位置、送信ストリームを測定します。

spectrum: スペクトル測定を指定します。スペクトル測定は、基本測定、CCA 測定（Clear Channel Assessment）、RPI 測定（Receive Power Indication）を実施します。

tpc: TPC 測定を指定します。TPC 測定は、リンク冗長性とクライアントへの送信電力を測定します。

disable: 指定された測定機能またはすべての測定機能を無効にします。

enable: 指定された測定機能またはっすべての測定機能を有効にします。

説明

measure enable コマンドは指定の測定機能もしくはすべての測定機能を有効にします。

measure disable コマンドは指定の測定機能もしくはすべての測定機能を無効にします。

undo measure コマンドはデフォルトに戻します。

link、**neighbor**、**radio** を有効にする場合は、**resource-measure** コマンドを有効にする必要があります。

spectrum、**tpc** を有効にする場合は、**spectrum-management** コマンドを有効にする必要があります。**spectrum-management** コマンドの詳細は、コマンドマニュアルのセクション 8 *Radio リソース管理 "スペクトル管理"* を参照してください。

spectrum、**tpc** は 5GHz のラジオでのみ使用できます。

例

無線測定を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] measure radio enable

関連コマンド

- **measure-duration**
- **measure-interval**
- **resource-measure**
- **spectrum-management**

2.1.3 measure-duration

Syntax

measure-duration *time*

undo measure-duration

デフォルト

500 TU

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

time: 測定期間を指定します。設定範囲は 1～10000TU です。1TU=1024 マイクロ秒です。

説明

measure-duration コマンドは測定期間を設定します。

undo measure-duration コマンドはデフォルトに戻します。

AP で測定が有効になると、AP からクライアントへの測定要求により測定期間を通知します。

例

測定期間を 512TU に指定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] measure-duration 512

関連コマンド

- **measure**
- **measure-interval**

2.1.4 measure-interval

Syntax

measure-interval *interval*

undo measure-interval

デフォルト

30 秒

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

interval: 測定間隔を指定します。設定範囲は 10～60 秒です。

説明

measure-interval コマンドは AP が測定要求をクライアントに送信するための測定間隔を設定します。

undo measure-interval コマンドはデフォルトに戻します。

例

AP ap1 の測定間隔を 35 秒に指定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] measure-interval 35

関連コマンド

- **measure**
- **measure-duration**

2.1.5 resource-measure

Syntax

resource-measure { **disable** | **enable** }

undo resource-measure

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: 無線リソース計測を無効にします。

enable: 無線リソース計測を有効にします。

説明

resource-measure enable コマンドは無線リソース計測を有効にします。

resource-measure disable コマンドは無線リソース計測を無効にします。

undo resource-measure コマンドはデフォルトに戻します。

AP で無線測定を有効にすると、AP はビーコン、プローブ応答、アソシエーション応答、再アソシエーション応答の Radio Measurement フィールドを 1 に設定し、計測要求を送信できることをクライアントに通知します。 また、このフレームで、AP がサポートする計測タイプをクライアントに通知します。

AP は定期的に Measurement Pilot フレームを送信して、クライアントが AP を高速に検出できるようにします。 Measurement Pilot フレームは、ビーコンよりも頻繁に送信され、より少ない情報しか運びません。

例

無線資源計測を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] resource-measure enable

2.1.6 rm-capability mode

Syntax

rm-capability mode { **all** | **none** | **partial** }

undo rm-capability mode

デフォルト

none

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

all: all モードを指定します。 クライアントは、すべての無線資源計測機能が AP の無線資源計測機能と一致する場合にのみ、AP に接続することができます。

none: none モードを指定します。 AP はクライアントの無線資源計測機能をチェックしません。

partial: 部分モードを指定します。 クライアントは、少なくとも 1 つの無線資源計測機能が AP の無線資源計測機能と一致する場合、AP に接続することができます。

説明

rm-capability mode コマンドはクライアント無線計測能力に対して一致モードを設定します。

undo rm-capability mode コマンドはデフォルトに戻します。

この設定は、無線資源計測が有効な場合にのみ有効です。

例

AP ap1 のクライアント無線資源計測機能を部分モードに指定します

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] rm-capability mode partial

関連コマンド

resource-measure

目次

このセクションのページは **6-x-x** です。

3 章 バンドナビゲーション 3-1
3.1 バンドナビゲーション設定コマンド 3-1
3.1.1 wlan band-navigation aging-time 3-1
3.1.2 wlan band-navigation balance access-denial 3-2
3.1.3 wlan band-navigation balance session 3-3
3.1.4 wlan band-navigation enable 3-4
3.1.5 wlan band-navigation rssi-threshold 3-5

3章 バンドナビゲーション

3.1 バンドナビゲーション設定コマンド

3.1.1 wlan band-navigation aging-time

Syntax

wlan band-navigation aging-time *aging-time*

undo wlan band-navigation aging-time

デフォルト

180 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: クライアント情報のエージングタイマを指定します。設定範囲は 10～600 秒です。

説明

wlan band-navigation aging-time コマンドはクライアント情報のエージングタイマを設定します。

undo wlan band-navigation aging-time コマンドはデフォルトに戻します。

AP がクライアントからアソシエーション要求を受信すると、AP はクライアントの情報を記録し、クライアント情報エージングタイマを開始します。 エージングタイマが満了する前に AP がプローブ要求またはアソシエーション要求をクライアントから受信しない場合、AP はクライアントの情報を削除します。

適切なクライアント情報のエージングタイムを設定して、クライアントの関連付けとシステムリソースの効率性を確保します。

例

クライアント情報のエージングタイマを 50 秒に指定します。

<AP> system-view

[AP] wlan band-navigation aging-time 50

3.1.2 wlan band-navigation balance access-denial

Syntax

wlan band-navigation balance access-denial *access-denial*
undo wlan band-navigation balance access-denial

デフォルト

5 GHz アソシエーション リクエストの拒否の最大数は 1 です。

View

System view

定義済みユーザロール

network-admin

パラメータ

access-denial: 5 GHz アソシエーション リクエストの拒否の最大数を 1 ～ 10 の範囲で指定します。

説明

wlan band-navigation balance access-denial を使用して、5 GHz アソシエーション リクエストの拒否の最大数を設定します。

undo wlan band-navigation balance access-denial を使用してデフォルトに戻します。

5 GHz 無線がクライアントを拒否する回数が指定された最大数に達すると、無線はクライアントのアソシエーション要求を受け入れます。

例

5GHz または 2.4GHz アソシエーション要求の最大拒否回数を 5 回に指定します。

<AP> system-view

[AP] wlan band-navigation balance access-denial 5

3.1.3 wlan band-navigation balance session

Syntax

wlan band-navigation balance session *session* [**gap** *gap*]

undo wlan band-navigation balance session

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

session: 5GHz の無線クライアント数のしきい値を指定します。設定範囲は 2～40 です。

gap: 5GHz と最も少ない無線のクライアント数の差のしきい値を指定します。設定範囲は 1～8 で、デフォルト値は 4 です。

説明

wlan band-navigation balance session コマンドはバンドナビゲーションにロードバランスを設定します。

undo wlan band-navigation balance session コマンドはデフォルトに戻します。

AP は、バンドナビゲーションを有効にしても負荷分散を有効にしない場合、デュアルバンドクライアントを 5GHz 無線に誘導します。

AP は、次の条件が満たされた場合にクライアントの 5GHz アソシエーション要求を拒否します。

- 5GHz 無線のクライアント数が、指定したしきい値に達した場合。
- 5GHz 無線のクライアント数と最も少ない無線クライアント数との差が、指定したしきい値に達した場合。

例

#バンドナビゲーションの負荷分散を有効にし、クライアント数のしきい値である、session、gap をそれぞれ 10 と 5 に設定します。

<AP> system-view

[AP] wlan band-navigation balance session 10 gap 5

3.1.4 wlan band-navigation enable

Syntax

wlan band-navigation enable

undo wlan band-navigation enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan band-navigation enable コマンドはバンドナビゲーションをグローバルで有効にします。

undo wlan band-navigation enable コマンドはデフォルトに戻します。

バンドナビゲーションを適用するために、クライアントが使用する無線サービスに対してクイックアソシエーションが無効であることを確認してください。

例

グローバルバンドナビゲーションを有効にします。

<AP> system-view

[AP] wlan band-navigation enable

関連コマンド

- **band-navigation**
- **quick-association enable**

3.1.5 wlan band-navigation rssi-threshold

Syntax

wlan band-navigation rssi-threshold *rssi-threshold*

undo wlan band-navigation rssi-threshold

デフォルト

15

View

System view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold: バンドナビゲーションの RSSI しきい値を指定します。設定範囲は 5～100 です。

説明

wlan band-navigation rssi-threshold コマンドは RSSI（Received Signal Strength Indicator）しきい値をバンドナビゲーションに設定します。

undo wlan band-navigation rssi-threshold コマンドはデフォルトに戻します。

複数の無線でクライアントを検出する可能性があります。 5GHz 無線は、クライアントの RSSI がバンドナビゲーション RSSI しきい値よりも低い場合、クライアントのアソシエーション要求を拒否します。

例

バンドナビゲーションの RSSI しきい値を 40 に指定します。

<AP> system-view

[AP] wlan band-navigation rssi-threshold 40

目次

このセクションのページは **6-x-x** です。

4 章 チャネルスキャン 4-1
4.1 チャネルスキャン設定コマンド 4-1
4.1.1 scan channel blacklist 4-1
4.1.2 scan channel whitelist 4-2
4.1.3 scan idle-time 4-3
4.1.4 scan max-service-time 4-4
4.1.5 scan scan-time 4-5

4章 チャネルスキャン

4.1 チャネルスキャン設定コマンド

4.1.1 scan channel blacklist

Syntax

scan channel blacklist *channel-list*

undo scan channel blacklist { *channel-list* | **all** }

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

channel-list: チャネル番号を指定します。設定範囲は 1～144 です。

all: チャネルスキャンブラックリストのすべてのチャネルを指定します。

説明

scan channel blacklist コマンドはチャネルスキャンブラックリストを設定します。

undo scan channel blacklist コマンドはチャネルスキャンブラックリストから特定のチャネルを削除します。

AP にチャネルスキャンブラックリストを設定すると、AP はブラックリストの稼働中でないチャネルをスキャンしません。同じ AP に対してホワイトリストとブラックリストの両方を設定することはできません。チャネルスキャンブラックリストを設定する前に、チャネルスキャンホワイトリストのチャネルをすべて消去してください。

例

チャネル 1 とチャネル 6 をチャネルスキャンブラックリストに追加します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] scan channel blacklist 1 6

4.1.2 scan channel whitelist

Syntax

scan channel whitelist *channel-list*

undo scan channel whitelist { *channel-list* | **all** }

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

channel-list: チャネル番号を指定します。設定範囲は 1～144 です。

all: チャネルスキャンホワイトリストのすべてのチャネルを指定します。

説明

scan channel whitelist コマンドはチャネルスキャンホワイトリストを設定します。

undo scan channel whitelist コマンドはチャネルスキャンホワイトリストから特定のチャネルを削除します。

AP にチャネルスキャンホワイトリストを設定すると、AP はホワイトリストの稼働中でないチャネルと稼働中のチャネルをスキャンします。同じ AP に対してホワイトリストとブラックリストの両方を設定することはできません。チャネルスキャンホワイトリストを設定する前に、チャネルスキャンブラックリストのチャネルをすべて消去してください。

例

チャネル 1 とチャネル 6 をチャネルスキャンホワイトリストに追加します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] scan channel whitelist 1 6

4.1.3 scan idle-time

Syntax

scan idle-time *idle-time*

undo scan idle-time

デフォルト

100 ミリ秒

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

idle-time: サービスアイドルタイムアウトを指定します。設定範囲は 60～5000 ミリ秒です。最大サービス期間より長く設定することはできません。

説明

scan idle-time コマンドはサービスアイドルタイムアウトタイマを設定します。

undo scan idle-time コマンドはデフォルトに戻します。

AP は、サービス期間中、指定したサービスアイドルタイムアウトが切れても、現在のサービス期間がスキャン期間を超えるまで、新しいスキャン期間を開始しません。

サービスアイドルタイムアウトは、ビーコン間隔の倍数でなければなりません。 ビーコン間隔より小さいサービスアイドルタイムアウトを設定すると、ビーコン間隔値をサービスアイドルタイムアウトとして使用します。

例

サービスアイドルタイムアウトを 500 ミリ秒に指定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] scan idle-time 500

関連コマンド

beacon interval

4.1.4 scan max-service-time

Syntax

scan max-service-time { *max-service-time* | **no-limit** }

undo scan max-service-time

デフォルト

5000 ミリ秒

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

max-service-time: 最大サービス期間を指定します。設定範囲は 100～5000 ミリ秒です。

no-limit: 無線がサービス期間を制限しないように設定します。 無線サービスの品質を確保するには、このキーワードを指定します。 サービスアイドルタイムアウトが切れるまで、AP はスキャン期間を開始しません。

説明

scan max-service-time コマンドは最大サービス期間を設定します。

undo scan max-service-time コマンドはデフォルトに戻します。

AP の最大サービス期間に達すると、AP は転送するトラフィックがあるかどうかにかかわらず、スキャン期間を開始します。

例

最大サービス期間を 3000 ミリ秒に指定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] scan max-service-time 3000

4.1.5 scan scan-time

Syntax

scan scan-time *scan-time*

undo scan scan-time

デフォルト

100 ミリ秒

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

scan-time: スキャン時間を指定します。設定範囲は 100～5000 ミリ秒です。スキャン期間は最大サービス期間より長くすることはできません。

説明

scan scan-time コマンドはスキャン期間を設定します。

undo scan scan-time コマンドはデフォルトに戻します。

例

スキャン期間を 500 ミリ秒に指定します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] scan scan-time 500

目次

このセクションのページは **6-x-x** です。

5 章 スペクトル管理 5-1
5.1 スペクトル管理コマンド 5-1
5.1.1 channel-capability mode 5-1
5.1.2 channel-switch mode 5-3
5.1.3 power-capability mode 5-4
5.1.4 power-constraint mode 5-5
5.1.5 spectrum-management 5-6

5章 スペクトル管理

5.1 スペクトル管理コマンド

5.1.1 channel-capability mode

Syntax

channel-capability mode { all | none | partial }

undo channel-capability mode

デフォルト

none

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

all: チャネルケーパビリティマッチモードの all モードを指定します。クライアントのサポートするチャネルが、無線のサポートするチャネルとすべて一致する場合のみ、クライアントは無線への紐付けが許可されます。

none: チャネルケーパビリティマッチモードの none モードを指定します。クライアントのチャネルケーパビリティはチェックされません。

partial: チャネルケーパビリティマッチモードの partial モードを指定します。クライアントのサポートするチャネルが､無線のサポートするチャネルと 1 つでも一致する場合、クライアントは無線への紐付けが許可されます。

説明

channel-capability mode コマンドはチャネルケーパビリティマッチモードを設定します。

undo channel-capability mode コマンドはデフォルトに戻します。

このコマンドは、5 GHz 無線でのみ使用できます。

この機能を使用する場合、スペクトル管理を有効にしてください。

無線ビューの設定は、AP グループの無線ビューの設定よりも優先されます。

例

Radio1 でチャネルケーパビリティマッチモードを all に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] spectrum-management enable

[AP-WLAN-Radio1/0/1] channel-capability mode all

5.1.2 channel-switch mode

Syntax

channel-switch mode { continuous | suspend }

undo channel-switch mode

デフォルト

suspend

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

continuous: チャネル切り替え中もフレームの送信を継続するようにオンラインクライアントを設定します。

suspend: チャネル切り替えが完了するまで、フレームの送信を停止するようにオンラインクライアントを設定します。

説明

channel-switch mode コマンドはチャネルスイッチモードを設定します。

undo channel-switch mode コマンドはデフォルトに戻します。

このコマンドは、5 GHz 無線でのみ使用できます。

この機能を使用する場合、スペクトル管理を有効にしてください。

無線ビューの設定は、AP グループの無線ビューの設定よりも優先されます。

例

Radio1 でチャネルスイッチモードを continuous に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] spectrum-management enable

[AP-WLAN-Radio1/0/1] channel-switch mode continuous

5.1.3 power-capability mode

Syntax

power-capability mode { all | none | partial }

undo power-capability mode

デフォルト

none

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

all: all モードを指定します。クライアントの伝送電力ケーパビリティが、無線の伝送電力ケーパビリティとすべて一致する場合のみ、クライアントは無線への紐付けが許可されます。

none: クライアントの伝送電力ケーパビリティはチェックされません。

partial: クライアントの伝送電力ケーパビリティが、無線の伝送電力ケーパビリティと 1 つでも一致する場合、クライアントは無線への紐付けが許可されます。

説明

power-capability mode コマンドはクライアント電力能力一致モードを設定します。

undo power-capability mode コマンドはデフォルトに戻します。

この機能を使用する場合、スペクトル管理を有効にしてください。

無線ビューの設定は、AP グループの無線ビューの設定よりも優先されます。

例

Radio 1 のクライアント電力能力一致モードを all に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] spectrum-management enable

[AP-WLAN-Radio1/0/1] power-capability mode all

5.1.4 power-constraint mode

Syntax

power-constraint mode { **auto** [**anpi-interval** *anpi-interval-value*] | **manual** *power-constraint* }

undo power-constraint mode

デフォルト

auto

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

auto: 自動モードを指定します。

anpi-interval anpi-interval-value:デバイスの平均ノイズ電力インジケータ (ANPI) に値を追加して、電力制約値を計算します。値の範囲は 0~30 (dBm) です。デフォルト値は 10 dBm です。

manual power-constraint: 電力制約値を 0~30 dBm の範囲で指定します。

説明

power-constraint mode コマンドは電力制約モードを設定します。

undo power-constraint mode コマンドはデフォルトに戻します。

このコマンドは、5 GHz 無線でのみ使用できます。

auto モードを指定すると、デバイスは次の式を使用して電力制約値を計算します。

電力制約値 = 受信チャネル電力インジケータ(RCPI) - (雑音電力及び干渉電力(ANPI) + ANPI 間隔値)

この機能を使用する場合、スペクトル管理もしくは無線リソース管理を有効にしてください。無線リソース管理の詳細は、オペレーションマニュアルのセクション 8 *Radio リソース管理 "WLAN 無線リソースの計測"* を参照してください。

無線ビューの設定は、AP グループの無線ビューの設定よりも優先されます。

例

Radio1 の電力制約値を 5 dBm に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] spectrum-management enable

[AP-WLAN-Radio1/0/1] power-constraint mode manual 5

5.1.5 spectrum-management

Syntax

spectrum-management { disable | enable }

undo spectrum-management

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

enable: スペクトル管理を有効にします。

disable: スペクトル管理を無効にします。

undo: スペクトル管理をデフォルトに戻します。

説明

spectrum-management enable コマンドはスペクトル管理を有効にします。

spectrum-management disable コマンドはスペクトル管理を無効にします。

undo spectrum-management コマンドはデフォルトに戻します。

このコマンドは、5 GHz 無線でのみ使用できます。

無線ビューの設定は、AP グループの無線ビューの設定よりも優先されます。

例

Radio1 のスペクトル管理を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] spectrum-management enable

QX-W610 アクセスポイント

コマンドマニュアル

07.WLAN アクセス

本マニュアルは以下に示す章で構成されています。

01-WLAN アクセス

目次

このセクションのページは **7-x-x** です。

1 章 WLAN アクセス 1-1
1.1 WLAN アクセス設定コマンド 1-1
1.1.1 access-control acl 1-1
1.1.2 beacon ssid-advertise 1-3
1.1.3 beacon ssid-hide 1-4
1.1.4 beacon ssid-advertise 1-5
1.1.5 client max-count 1-6
1.1.6 client smart-access enable 1-7
1.1.7 customlog format wlan 1-8
1.1.8 description 1-10
1.1.9 display interface wlan-radio 1-11
1.1.10 display wlan ap all client-number 1-15
1.1.11 display wlan ap all radio client-number 1-16
1.1.12 display wlan blacklist 1-17
1.1.13 display wlan bss 1-19
1.1.14 display wlan client 1-21
1.1.15 display wlan client device-information 1-29
1.1.16 display wlan client failure 1-31
1.1.17 display wlan client online-duration 1-33
1.1.18 display wlan client status 1-34
1.1.19 display wlan service-template 1-37
1.1.20 display wlan statistics client 1-43
1.1.21 display wlan statistics connect-history 1-46
1.1.22 display wlan statistics service template 1-47
1.1.23 display wlan whitelist 1-48
1.1.24 interface wlan-radio 1-49
1.1.25 nas-id 1-50
1.1.26 nas-port-type 1-51
1.1.27 quick-association enable 1-53
1.1.28 reset wlan client 1-54
1.1.29 reset wlan dynamic-blacklist 1-55
1.1.30 reset wlan statistics client 1-56
1.1.31 reset wlan statistics service-template 1-57
1.1.32 service-template 1-58
1.1.33 service-template enable 1-59
1.1.34 snmp-agent trap enable wlan client 1-60

1.1.35 ssid 1-61
1.1.36 unknown-client 1-63
1.1.37 vip limit rate 1-64
1.1.38 vlan 1-66
1.1.39 wlan association optimization 1-67
1.1.40 wlan broadcast-probe reply 1-68
1.1.41 wlan client bss-load-ie enable 1-69
1.1.42 wlan client failure history aging 1-70
1.1.43 wlan client idle-timeout 1-71
1.1.44 wlan client keep-alive 1-72
1.1.45 wlan client keep-alive interval 1-73
1.1.46 wlan client reauthentication-period 1-74
1.1.47 wlan dynamic-blacklist lifetime 1-75
1.1.48 wlan link-test 1-76
1.1.49 wlan nas-port-id format 1-78
1.1.50 wlan service-template 1-79
1.1.51 wlan static-blacklist mac-address 1-80
1.1.52 wlan web-server api-path 1-81
1.1.53 wlan web-server host 1-82
1.1.54 wlan web-server max-client-entry 1-83
1.1.55 wlan whitelist mac-address 1-84

1章 WLAN アクセス

1.1 WLANアクセス設定コマンド

1.1.1 access-control acl

Syntax

access-control acl *acl-number*

undo access-control acl

デフォルト

設定無し

View

Service template view

定義済みユーザロール

network-admin

パラメータ

acl-number: レイヤ 2 ACL の番号を 4000 から 4999 の範囲で指定します。

説明

access-control acl コマンドは ACL にもとづくアクセスに使用する ACL を設定します。

undo access-control acl コマンドはデフォルトに戻します。

この機能は、指定された ACL ルールを使用してクライアントアクセスを制御します。デバイスはアソシエーション要求を受信すると、次のアクションを実行します。

- クライアントの MAC アドレスがルール内の MAC アドレス属性または MAC アドレス OUI 属性と一致し、ルールアクションが permit の場合に、クライアントに WLAN へのアクセスを許可します。複数のクライアントが OUI 属性に一致する場合、これらのすべてのクライアントは WLAN へのアクセスを許可されます。
- 一致するルールが見つからない場合、または一致するルールのアクションが deny の場合、クライアントの WLAN へのアクセスを拒否します。

この機能を設定する場合は、次の制約事項および注意事項に従ってください。

- 指定した ACL に permit ルールが設定されていない場合、クライアントのアクセスは許可されません。
- 指定できる ACL は 1 つだけです。このコマンドを複数回実行した場合は、最新の設定が有効になります。

例

ACL 4000 を作成し、MAC アドレスが 006e-35b2-000e のクライアントおよび指定された OUI のクライアントアクセスを許可する ACL ルールを作成します。サービステンプレート service 1 に ACL4000 を指定します。

<AP> system-view

[AP] acl mac 4000

[AP -acl-mac-4000] rule 0 permit source-mac 006e-35b2-000e ffff-ffff-ffff

[AP -acl-mac-4000] rule 1 permit source-mac 006e-3500-0000 ffff-ff00-0000

[AP -acl-mac-4000] quit

[AP] wlan service-template service1

[AP -wlan-st-service1] access-control acl 4000

1.1.2 beacon ssid-advertise

Syntax

beacon ssid-advertise

undo beacon ssid-advertise

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

beacon ssid-advertise コマンドはビーコンフレームで Service Set Identifier (SSID) ブロードキャストを有効にします。

undo beacon ssid-advertise コマンドはデフォルトに戻します。

この機能により、関連付けられているクライアントの数が上限に達した場合でも、新しいクライアントは AP を検出できます。ただし、これらのクライアントは AP と関連付けることができません。

例

ビーコンフレームでの SSID ブロードキャストを有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-s1] beacon ssid-advertise

関連コマンド

client max-count

1.1.3 beacon ssid-hide

Syntax

beacon ssid-hide

undo beacon ssid-hide

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

beacon ssid-hide コマンドは SSID ステルスを有効にします。

undo beacon ssid-hide コマンドはデフォルトに戻します。

このコマンドを有効にすると、無線がビーコンフレーム内で SSID を伝送しないようになり、指定したサービステンプレートが無線にバインドされた後にプローブ要求に応答しなくなります。

例

SSID ステルスを有効(ビーコンフレームの SSID 通知を無効)にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] beacon ssid-hide

1.1.4 beacon ssid-advertise

Syntax

beacon ssid-advertise

undo beacon ssid-advertise

デフォルト

クライアントの最大数に達すると、ビーコンフレーム内の SSID を非表示にします。

View

Service template view

定義済みユーザロール

network-admin

説明

beacon ssid-advertise コマンドはビーコンフレーム内の Service Set Identifier (SSID) ブロードキャストを有効にします。

undo beacon ssid-advertise コマンドはデフォルトに戻します。

この機能により、関連付けられているクライアントの数が上限に達した場合でも、新しいクライアントが AP を検出できます。ただし、これらのクライアントは AP と関連付けることができません。

例

ビーコンフレームでの SSID ブロードキャストを有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-s1] beacon ssid-advertise

関連コマンド

client max-count

1.1.5 client max-count

Syntax

client max-count *max-number*

undo client max-count

デフォルト

制限なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

max-number: クライアントの最大数を指定します。設定範囲は 1～512 です。

説明

client max-count コマンドはサービステンプレートに紐付けるクライアントの最大数を指定します。

undo client max-count コマンドはデフォルトに戻します。

この機能が設定されている場合、最大数に達していると新たなクライアントは WLAN にアクセスできません。

例

サービステンプレート service1 に紐付くクライアントの最大数を 38 に設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] client max-count 38

1.1.6 client smart-access enable

Syntax

client smart-access enable

undo client smart-access enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

mdc-admin

説明

client smart-access enable コマンドはスマートクライアントアクセスを有効にします。

undo client smart-access enable コマンドはデフォルトに戻します。

この機能により、AKM モードが PSK に設定されている場合、または無線が空のサービステンプレートにバインドされている場合に、H３C 無線クライアントが自動的に WLAN にアクセスできるようになります。

例

スマートクライアントアクセスを有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-s1] client smart-access enable

1.1.7 customlog format wlan

Syntax

customlog format wlan { **normal** | **sangfor** }

undo customlog format wlan

デフォルト

normal

View

System view

定義済みユーザロール

network-admin

パラメータ

normal: 通常フォーマットを指定します。

sangfor: sangfor 形式を指定します。

説明

customlog format wlan コマンドは、装置が指定された形式のクライアントログを生成します。

undo customlog format wlan コマンドはデフォルトに戻します。

デフォルトでは、装置は AP 名、無線 ID、クライアント MAC アドレス、SSID、BSSID、およびクライアントのオンラインステータスを記録するNEC形式のクライアントログのみを生成します。

次のいずれかの形式でクライアントログを生成するように装置を設定できます。

- **normal**−AP MAC アドレス、AP 名、クライアント IP アドレス、クライアント MAC アドレス、SSID、および BSSID を記録します。
- **sangfor**−AP の MAC アドレス、クライアントの IP アドレス、およびクライアントの MAC アドレスを記録します。

この機能は、NEC 形式のクライアントログの生成には影響しません。

例

#装置が sangfor 形式でクライアントログを生成できるようにします。

<AP> system-view

[AP] customlog format wlan sangfor

1.1.8 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

text: description 名を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

description コマンドはサービステンプレートの説明を設定します。

undo description コマンドはデフォルトに戻します。

例

サービステンプレート service1 に description 名 wlanst を指定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] description wlanst

1.1.9 display interface wlan-radio

Syntax

display interface wlan-radio [*interface-number*] [**brief**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-number: WLAN 無線インタフェースを指定します。指定しない場合、すべての WLAN 無線インタフェースの情報を表示します。

brief: インタフェースの概要を表示します。指定しない場合、詳細な情報を表示します。

説明

display interface wlan-radio コマンドは WLAN 無線インタフェースの状態を表示します。

例

WLAN 無線インタフェース 1/0/1 の詳細情報を表示します。

<AP> display interface wlan-radio 1/0/1

```
WLAN-Radio1/0/1
Current state: UP
Description: WLAN-Radio1/0/1 Interface
IP Packet Frame Type: PKTFMT_IEEE_802.11, Hardware Address: d461-fe59-4d20
current mode: 802.11ac, current channel: 36
Last link flapping: 0 hours 31 minutes 6 seconds
Last clearing of counters: Never
Current system time:2016-01-01 00:31:19
Last time when physical state changed to up:2016-01-01 00:00:13
Last time when physical state changed to down:2016-01-01 00:00:13
Input (total): 0 packets, 0 bytes
Input (normal): 0packets, 0bytes
              0 management, 0 control, 0 data
Input (error): 0 total, 0 CRC, 0 decrypt errors
             0 mic failures, 0 phy errors, 0 other errors
Output (total): 0 packets, 0 bytes
Output (normal): Q[0]:0, Q[1]:0, Q[2]:0, Q[3]:0 packets
               Q[0]:0, Q[1]:0, Q[2]:0, Q[3]:0 bytes
```

```
                0 management, 0 control, 0 data
Output (bcn&probe): 0 packets, 0 bytes
Output (error): 0 total, 0 discard, 0 buffer failures
             0 ack failures, 0 rts successed, 0 rts failures
```

表 1-1 コマンド出力

フィールド	説明
Current state	インタフェースのリンク状態です。 • **UP**—インタフェースが物理的にUPしています。 • **DOWN**—インタフェースが物理的にDOWNしています。 • **ADM**—インタフェースがシャットダウンしています。UPにする場合、**undo shutdown**コマンドを実行します。 • **Stby**—インタフェースがバックアップインタフェースです。
IP Packet Frame Type	PKTFMT_IEEE_802.11を表示します。802.11がカプセル化されていることを示します。
Hardware Address	インタフェースのMACアドレスです。
current mode	現在の無線モードです。
current channel	現在の動作チャネルです。
Last link flapping	インタフェースの物理状態が最後に変更してからの経過時間です。**Never**は装置が起動してから物理的にダウンしていないことを示します。
Last clearing of counters	**reset counters interface**コマンドを使用してインタフェースの統計情報を最後に削除してからの経過時間です。**Never**は装置が起動してから**reset counters interface**コマンドを使用していないことを示します。
Current system time	現在のシステム時間です。形式はYYYY/MM/DD HH:MM:SSです。タイムゾーンが設定されている場合、HH:MM:SS UTC±HH:MM:SSの形式で表示されます。
Last time when physical state changed to up	インタフェースの物理状態が最後にUPになった時間です。“-”は装置が起動してから物理状態が変更されていないことを示します。
Last time when physical state changed to down	インタフェースの物理状態が最後にDOWNになった時間です。“-”は装置が起動してから物理状態が変更されていないことを示します。
Input(total): 0 packets, 0 bytes	インタフェースの受信パケットの統計情報です。単位はパケット数、バイトです。すべての正常なパケットと異常なパケットがカウントされます。

フィールド	説明
Input (normal): 0packets, 0bytes 0 management, 0 control, 0 data	インタフェースの正常な受信パケットの統計情報です。単位はパケット数、バイトです。すべての管理、制御、データがカウントされます。
Input (error)	インタフェースの受信エラーパケットの統計情報です。
Output (total): 0 packets, 0 bytes	インタフェースの送信パケットの統計情報です。単位はパケット数、バイトです。すべての正常なパケットと異常なパケットがカウントされます。
Output (normal): Q[0]:0, Q[1]:0, Q[2]:0, Q[3]:0 packets Q[0]:0, Q[1]:0, Q[2]:0, Q[3]:0 bytes 0 management, 0 control, 0 data	インタフェースの正常な送信パケットの統計情報です。単位はパケット数、バイトです。すべての管理、制御、データがカウントされます。 **Q[*n*]**はACのキューを示します。*n*はキューIDです。
Output (bcn&probe)	インタフェースの送信ビーコン、プローブフレームの統計情報です。単位はパケット数、バイトです。
Output (error)	インタフェースの送信エラーパケットの統計情報です。

WLAN 無線インタフェース 1/0/1 の概要情報を表示します。

<AP> display interface wlan-radio 1/0/1

```
Brief information on interfaces in bridge mode:
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed    Duplex Type PVID Description
WLAN-Radio1/0/1       UP   --       --    --   --
```

表 1-2 コマンド出力

フィールド	説明
Brief information on interfaces in bridge mode	レイヤ2インタフェースの概要情報です。
Link	インタフェースのリンク状態です。 • **UP**—インタフェースが物理的にUPしています。 • **DOWN**—インタフェースが物理的にDOWNしています。 • **ADM**—インタフェースがシャットダウンしています。UPにする場合、**undo shutdown**コマンドを実行します。 • **Stby**—インタフェースがバックアップインタフェースです。

フィールド	説明
Speed	インタフェースの通信速度です。単位はMbpsです。 インタフェースが自動でネゴシエーションされる場合、(a)で示されたオートネゴシエーションのフラグが含まれます。 WLAN無線インタフェースは“--”と表示します。
Duplex	インタフェースの通信モードです。 ● **(a)/A**—オートネゴシエーションです。 ● **H**—通信モードがhalfです。 ● **F**—通信モードがfullです。 WLAN無線インタフェースは“--”と表示します。
Type	インタフェースのリンクタイプです。 ● **A**ーアクセスです。 ● **H**ーハイブリッドです。 ● **T**ートランクです。 WLAN無線インタフェースは“--”と表示します。

関連コマンド

interface wlan-radio

1.1.10 display wlan ap all client-number

Syntax

display wlan ap all radio client-number

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap all radio client-number コマンドは、2.4 GHz 帯域と 5 GHz 帯域のオンラインクライアントの数が表示します。

例

2.4 GHz 帯域と 5 GHz 帯域の両方のオンラインクライアントの数を表示します。

<AP> display wlan ap all client-number

```
AP name       Clients          2.4GHz       5GHz
fatap         2                2            0
```

表 1-3 コマンド出力

フィールド	説明
Clients	オンラインクライアントの総数です。
2.4GHz	2.4 GHz帯域のオンラインクライアントの数です。
5GHz	5GHz帯域のオンラインクライアントの数です。

1.1.11 display wlan ap all radio client-number

Syntax

display wlan ap all radio client-number

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan ap all radio client-number コマンドは、各無線のオンラインクライアント数とチャネル情報が表示します。

例

各無線のオンラインクライアント数とチャネル情報を表示します。

<AP> display wlan ap all radio client-number

```
AP name                  RID     Channel     Clients
fatap                    1           44             12
fatap                    2           11             4
```

1.1.12 display wlan blacklist

Syntax

display wlan blacklist { **dynamic** | **static** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dynamic: 動的なブラックリストを指定します。

static: 静的なブラックリストを指定します。

説明

display wlan blacklist コマンドはブラックリストエントリを表示します。

例

静的なブラックリストエントリを表示します。

<AP> display wlan blacklist static

```
Total number of clients: 3
 MAC addresses:
  000e-35b2-000e
  0019-5b8e-b709
  001c-f0bf-9c92
```

動的なブラックリストエントリを表示します。

<AP> display wlan blacklist dynamic

```
Total number of clients: 3
MAC address    APID  Lifetime (s)  Duration (hh:mm:ss)
000f-e2cc-0001  1    300           00:02:11
000f-e2cc-0002  2    300           00:01:17
000f-e2cc-0003  3    300           00:02:08
```

表 1-4 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
APID	不正なクライアントを検出したAPのID。

フィールド	説明
Lifetime (s)	エントリの寿命（秒単位）。
Duration (hh:mm:ss)	エントリが動的ブラックリストに追加されてからエントリ期間。

1.1.13 display wlan bss

Syntax

display wlan bss { **all** | **bssid** *bssid* } [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべての BSS を表示します。

bssid *bssid*: BSS を ID で指定します。ID は、48 ビットの 16 進数で H-H-H の形式で指定してください。

verbose: 詳細な BSS 情報を表示します。 このキーワードを指定しない場合、BSS 情報の概要を表示します。

説明

display wlan bss コマンドは BSS（Basic Service Set）情報を表示します。

例

すべての BSS の簡潔な情報を表示します。

<AP> display wlan bss all

```
Current BSS number: 4
AP name                RID  SSID                      BSSID
fatap                   1   SSID1                     0f00-ef65-6400
fatap                   2   SSID1                     0f00-ef65-6401
fatap                   1   SSID1                     0f00-ef14-dd08
fatap                   2   SSID1                     0f00-ef14-dd09
```

ID が 0f00-ef65-6400 の BSS の詳細情報を表示します。

<AP> display wlan bss bssid 0f00-ef65-6400 verbose

```
AP name                   : fatap
BSSID                     : 0f00-ef65-6400
Radio ID                  : 1
Service template name     : servcie1
SSID                      : SSID1
VLAN ID                   : 1
Service VLAN ID           : N/A
```

```
AKM mode                  : Not configured
User authentication mode  : Bypass
```

表 1-5 コマンド出力

フィールド	説明
AKM mode	AKMモード： ● 802.1X ● PSK ● 設定なし
User authentication mode	ユーザ認証モード： ● **Bypass**ークライアント認証なし ● **MAC** ● **802.1X** ● **OUI**

1.1.14 display wlan client

Syntax

display wlan client [**interface wlan-radio** *interface-number* | **mac-address** *mac-address* | **service-template** *service-template-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

wlan-radio *interface-number*: 指定した無線インタフェースに接続されているクライアントに関する情報を表示します。

mac-address *mac-address*: クライアントを MAC アドレスで指定します。

service-template *service-template-name*: 指定したサービステンプレートに関連付けられているクライアントに関する情報を表示します。 サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

verbose: 詳細なクライアント情報を表示します。 このキーワードを指定しない場合、クライアント情報の概要を表示します。

説明

display wlan client コマンドはクライアント情報を表示します。

例

すべてのクライアントに関する簡潔なクライアント情報を表示します。

<AP> display wlan client

```
Total number of clients: 3

MAC address    Username        AP name      RID   IP address         VLAN
000f-e265-6400 N/A             fatap        1     1.1.1.1            100
000f-e265-6401 user            fatap        1     3.0.0.3            200
000f-e214-dd08 N/A             fatap        1     5.5.5.3            1
```

表 1-6 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。

フィールド	説明
Username	クライアントユーザ名 ● クライアントのユーザ名（802.1X認証またはMAC認証を使用している場合） ● **N/A**（802.1X認証またはMAC認証を使用していない場合） 🕮 **メモ：** クライアントがポータル認証を使用する場合、このフィールドにクライアントのポータルユーザ名は表示されません。
AP name	クライアントが紐付けられたAPの名前。
RID	クライアントが接続している無線のID。
IPv4 address	クライアントのIPv4アドレス。
IPv6 address	クライアントのIPv6アドレス。
VLAN ID	クライアントが属するVLANのID。

すべてのクライアントに関する詳細なクライアント情報を表示します。

<AC> display wlan client verbose

```
Total number of clients: 1

 MAC address                    : 000f-e265-6400
 IPv4 address                   : 10.1.1.114
 IPv6 address                   : 2001::1234:5678:0102:0304
 Username                      : N/A
 AID                           : 1
 Radio ID                       : 1
 Channel                        : 36
 SSID                          : office
 BSSID                         : 882a-5e6c-4e60
 VLAN ID                        : 1
 Service VLAN ID                 : N/A
 Sleep count                    : 2
 Wireless mode                  : 802.11ac
 Channel bandwidth               : 80MHz
 SM power save                  : Disabled
 Short GI for 20MHz              : Supported
 Short GI for 40MHz              : Supported
 Short GI for 80MHz              : Supported
```

```
Short GI for 160/80+80MHz        : Not supported
STBC RX capability               : Supported
STBC TX capability               : Supported
LDPC RX capability               : Supported
Beamformee STS capability        : N/A
Number of Sounding Dimensions    : N/A
SU beamformee capability         : Not supported
MU beamformee capability         : Not supported
Block Ack                        : N/A
Supported VHT-MCS set            : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
                                   NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set             : 0, 1, 2, 3, 4, 5, 6, 7,
                                   8, 9, 10, 11, 12, 13, 14,
                                   15
Supported rates                  : 6, 9, 12, 18, 24, 36,
                                   48, 54 Mbps
QoS mode                         : WMM
Listen interval                  : 250
RSSI                             : 38
Rx/Tx rate                       : 780/6 Mbps
Speed                            : 0.384/0.024Kbps
Authentication method            : Open system
Security mode                    : RSN
AKM mode                         : PSK
Cipher suite                     : CCMP
User authentication mode         : Bypass
WPA3 status                      : Disabled
Authorization CAR                : N/A
Authorization ACL ID             : N/A
Authorization user profile       : N/A
Roam status                      : N/A
Key derivation                   : SHA1
PMF status                       : N/A
Forwarding policy name           : Not configured
Online time                      : 0days 0hours 0minutes 40seconds
FT status                        : Inactive
BTM mode                         : Inactive
```

表 1-7 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。

フィールド	説明
IPv4 address	クライアントIPv4アドレス。
IPv6 address	クライアントIPv6アドレス。
Username	クライアントユーザ名 ● クライアントのユーザ名（802.1X認証またはMAC認証を使用している場合） ● **N/A**（802.1X認証またはMAC認証を使用していない場合） 🕮 **メモ：** クライアントがポータル認証を使用する場合、このフィールドにクライアントのポータルユーザ名は表示されません。
AID	アソシエーションID。
AP ID	クライアントが接続しているAPのID。
AP name	クライアントが接続しているAPの名前。
Radio ID	クライアントが接続している無線のID。
SSID	クライアントが接続しているSSID。
VLAN ID	クライアントが属するVLANのID。
Sleep count	スリープ状態への遷移数。
Wireless mode	無線モードを示します。 ● 802.11a. ● 802.11b. ● 802.11g. ● 802.11gn. ● 802.11an. ● 802.11ac. ● 802.11ax.
Channel bandwidth	チャネル帯域幅を示します。 20MHz、40MHz、80MHz、160MHzです。
20/40 BSS Coexistence Management	クライアントが20/40MHzチャネル帯域幅の共有をサポートしているかどうかを示します。このフィールドは802.11nのみサポートします。

フィールド	説明
SM Power Save	SM Power Saveは、クライアントの1つのアンテナだけをアクティブ状態、他のものはスリープ状態で動作させ、電力を節約することを可能にします。 ● **Enabled**–有効 ● **Disabled**–無効
SM power save mode	省電力モード。 ● Dynamic. ● Static.
Short GI for 20MHz	チャネル帯域幅が20MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
Short GI for 40MHz	チャネル帯域幅が40MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
Short GI for 80MHz	チャネル帯域幅が80MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
Short GI for 160/80+80MHz	チャネル帯域幅が160/80+80MHzのときにクライアントがショートGIをサポートするかどうか。 ● Supported. ● Not supported.
STBC Rx Capability	クライアントSTBC受信能力 ● Not supported. ● Supported.
STBC Tx Capability	クライアントSTBC送信能力 ● Not supported. ● Supported.
LDPC Rx capability	クライアントLDPC受信能力 ● Not supported. ● Supported.
SU beamformee capability	クライアントSU beamformee 能力 ● Not supported. ● Supported. このフィールドは802.11ac/ax無線でのみサポートします。

フィールド	説明
MU beamformee capability	クライアントMU beamformee 能力 ● Not supported. ● Supported. このフィールドは802.11ac/ax無線でのみサポートします。
Beamformee STS capability	クライアントがbeamformeeレシーバである場合、サポートされる空間のストリーム量です。範囲は0～7です。（最大空間ストリーム量はMIMOモードー1で指定されます。） クライアントはbeamformeeレシーバとして動作することができない場合、N/Aと表示されます。 このフィールドは802.11ac/ax無線でのみサポートします。
Number of Sounding Dimensions	クライアントがbeamformeeトランスミッタである場合、サポートされる空間のストリーム量です。範囲は0～7です。（最大空間ストリーム量はMIMOモードー1で指定されます。） クライアントはbeamformeeトランスミッタとして動作することができない場合、N/Aと表示されます。 このフィールドは802.11ac/ax無線でのみサポートします。
Block Ack	TIDを用いたブロックアックのネゴシエーション結果。 ● **IN**–受信方向からトラフィックのブロックアックを送信します。 ● **OUT**–送信方向からトラフィックのブロックアックを送信します。 ● **BOTH**–送受信方向からトラフィックのブロックアックを送信します。 ● **N/A**ー送受信方向からトラフィックのブロックアックを送信しません。
Supported VHT-MCS set	クライアントによってサポートされたVHT-MCS
Supported HT MCS set	クライアントによってサポートされたHT-MCS
QoS mode	QoS モード。 ● **N/A**–WMMに対応しません。 ● **WMM**–WMMに対応します。 WMM情報ネゴシエーションは、WMMをサポートするAPとクライアントの間で実行されます。
Listen interval	クライアントがビーコンフレームを受信するためにウェイクアップする間隔。 ビーコン間隔でカウントされます。
RSSI	受信した信号強度の表示。 この値は、APによって検出されたクライアントの信号強度を示します。
Rx/Tx rate	データ、管理、制御フレームの送信および受信レート。

フィールド	説明
Speed	過去2分間の送受信レートを示します。単位は、Kbps です。小数点以下3桁で四捨五入しています。 N/A：送信レートと受信レートの両方が0の場合を示します。
Authentication method	認証方式を示します。 ● オープンシステム ● 共有鍵
Security mode	セキュリティモードを示します。 ● **RSN**：ビーコンおよびプローブ応答はRSN IEを伝送します。 ● **WPA**：ビーコンおよびプローブ応答はWPA IEを伝送します。 ● **PRE-RSNA**：ビーコンおよびプローブ応答はRSN IE/WPA IEを伝送しません。
AKM mode	AKMモードを示します。 ● 802.1X ● PSK ● Not configured.
Cipher suite	暗号スイートを示します。 ● N/A ● WEP40 ● WEP104 ● WEP128 ● CCMP ● TKIP
User authentication mode	ユーザ認証モードを示しています。 ● **Bypass**：クライアント認証なし。 ● **MAC**：MAC認証です。 ● **802.1X**：802.1X認証です。 ● **OUI**：OUI認証です。
Authorization ACL ID	許可されたACL番号を表示します。 ● ACL番号：許可されたACLが有効になった場合 ● ACL番号 + **Not effective**：許可されたACLが無効になった場合 ● **N/A**：許可されたACLがない場合
Authorization user profile	許可されたユーザープロファイル名を表示しています。 ● 許可されたユーザープロファイル名：許可されたACLが有効になった場合 ● 許可されたユーザープロファイル名 + **Not effective**：許可されたACLが無効になった場合 ● **N/A**：許可されたユーザープロファイルがない場合

フィールド	説明
Roam status	Roaming statusはローミングのステータスを示します。 ● Roaming in progress.：ローミング中です。 ● Inter-AP roam：AP間でローミングしました。 ● Intra-AP roam：AP内でローミングしました。 ● N/A：クライアントがオンラインになったものの、１つの BSS に留まっている状態です
Key derivation	キー派生タイプを示します。 ● **SHA1**：HMAC-SHA1ハッシュアルゴリズムを使用します。 ● **SHA256**：HMAC-SHA256ハッシュアルゴリズムを使用します。 ● **N/A**：アルゴリズムを使用しません。
PMF status	PMFのステータスを示します。 ● **Enabled**：管理フレーム保護が有効になっています。 ● **Disabled**：管理フレーム保護が無効になっています。 ● **N/A**：管理フレームの保護は行われません。
Forward policy	WLAN転送ポリシを示します。 ● **Not configured**：WLAN転送ポリシーが設定されていません。 ● *policy-name*.
Online time	クライアントのオンライン期間を示します。
FT status	FT (Fast BSS transition) のステータスを示します。 ● **Active**：有効 ● **Inactive**：無効
BTM mode	BTM (BSS transition management) を示します。 ● **Active**：有効 ● **Inactive**：無効

1.1.15 display wlan client device-information

Syntax

display wlan client device-information [mac-address *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

説明

オンラインになれなかったクライアントに関する情報を表示するには、**wlan client failure** を使用します。

デバイスは、最大 512 個のクライアント アソシエーション失敗レコードを保存できます。レコード数がこの上限を超えると、システムは最も古いレコードを自動的に削除します。

例

オンラインにできなかったクライアントに関する情報を表示します。

```
association failures: 0
authentication failures: 1
-----------
 Association failures:
 Client-info                       AP name    R SSID    Time

 Authentication failures:
 Client-info                       AP name    R SSID    Time
 8AE6-6CBB-AF91/-(-)                 1451-7e0f- 3 anchor-1 2021-06-09 12:17:26
                                   50c0        x-nec
```

表 1-8 コマンド出力

フィールド	説明
Client-info	オンラインにできなかったクライアントの MAC アドレスまたは IP アドレス (ユーザ名)。 オンラインに失敗したクライアントの MAC アドレスまたは IP アドレス (ユーザ名) を取得できなかった場合、システムはハイフン (-) を表示します。
AP name	クライアントがオンラインになろうとした AP の名前。
R	クライアントが関連付けられている radio ID。
SSID	クライアントが関連付けられている SSID。
Time	クライアントがオンラインになれなかった時間。

1.1.16 display wlan client failure

Syntax

display wlan client failure

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: クライアントの詳細な状況を表示します。このパラメータを指定しない場合、クライアントの概要状況を表示します。

説明

display wlan client status コマンドはクライアントのオンライン期間を表示します。

例

クライアントのオンライン期間に関する簡単な情報を表示します。

<AP> display wlan client online-duration

```
Total number of online clients: 2
MAC address           IPv4 address        Online duration
a4c1-5b79-fa5b-1d62   192.168.11.123      0days 0hours 2minutes 23seconds
22d3-c5b7-a4b5-96fa   192.168.11.234      0days 0hours 5minutes 34seconds
```

表 1-9 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
IPv4 address	クライアントIPv4アドレス。
IPv6 address	クライアントIPv6アドレス。

-
-
-
-
-
-

-

1.1.17 display wlan client online-duration

Syntax

display wlan client online-duration [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

verbose: クライアントの詳細な状況を表示します。このパラメータを指定しない場合、クライアントの概要状況を表示します。

説明

display wlan client status コマンドはクライアントのオンライン期間を表示します。

例

クライアントのオンライン期間に関する簡単な情報を表示します。

<AP> display wlan client online-duration

```
Total number of online clients: 2
MAC address           IPv4 address        Online duration
a4c1-5b79-fa5b-1d62   192.168.11.123      0days 0hours 2minutes 23seconds
22d3-c5b7-a4b5-96fa   192.168.11.234      0days 0hours 5minutes 34seconds
```

表 1-10 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
IPv4 address	クライアントIPv4アドレス。
IPv6 address	クライアントIPv6アドレス。

1.1.18 display wlan client status

Syntax

display wlan client status [**mac-address** *mac-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H 形式で指定します。このオプションを指定しない場合、すべてのクライアントの状況を表示します。

verbose: クライアントの詳細な状況を表示します。このパラメータを指定しない場合、クライアントの概要状況を表示します。

説明

display wlan client status コマンドはクライアントの状況を表示します。

例

特定のクライアントの状況を表示します。

<AP> display wlan client status mac-address 001c-f08f-f804

```
Total number of clients: 1

MAC address    Access time  RSSI  Rx/Tx rate     Discard  AP name         RID
001c-f08f-f804  41ms        0    39/117Mbps     0.00    fatap          2
```

すべてのクライアントの概要状況を表示します。

<AP> display wlan client status

```
Total number of clients: 2

MAC address    Access time  RSSI  Rx/Tx rate     Discard  AP name         RID
000b-c002-9d09  41ms        65    39/117Mbps     0.00%    fatap          2
000f-e265-6401  10ms        62    130/195Mbps     0.00%   fatap          1
```

表 1-11 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。

フィールド	説明
Access time	クライアントがWLANに紐付く時間
RSSI	クライアントのRSSI
Rx/Tx rate	クライアントがデータ、管理パケット、制御パケットを送受信する速度
Discard	クライアントに廃棄されるパケットの割合
AP name	クライアントが紐付いたAPの名前
RID	クライアントが紐付いた無線のID

特定のクライアントの詳細な状況を表示します。

<AP> display wlan client status mac-address 001c-f08f-f804 verbose

```
Total number of clients: 1

MAC address                    : 001c-f08f-f804
AP name                        : fatap
Radio ID                       : 2
Access time                    : 41 ms
RSSI                           : 0
Rx/Tx rate                     : 39/117 Mbps
Received:
 Retransmitted packets           : 84
 Retransmitted packet ratio      : 64.12%
Sent:
 Retransmitted packets           : 0
 Retransmitted packet ratio      : 0.00%
Discarded:
 Discarded packets               : 0
 Discarded packet ratio          : 0.00%
```

表 1-12 コマンド出力

フィールド	説明
MAC address	クライアントMACアドレス。
AP name	クライアントが紐付いたAPの名前
Radio ID	クライアントが紐付いた無線のID

フィールド	説明
Access time	クライアントがWLANに紐付く時間
RSSI	クライアントのRSSI
Rx/Tx rate	クライアントがデータ、管理パケット、制御パケットを送受信する速度
Received	受信パケット統計情報 ● 再伝送パケット ● 再伝送パケット比率
Sent	送信パケット統計情報 ● 再伝送パケット ● 再伝送パケット比率
Discarded	廃棄パケット統計情報 ● 廃棄パケット ● 廃棄パケット比率

1.1.19 display wlan service-template

Syntax

display wlan service-template [*service-template-name*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。この引数を指定しない場合、すべてのサービステンプレートに関する情報が表示されます。

verbose: 詳細なサービステンプレート情報を表示します。

説明

display wlan service-template コマンドはサービステンプレート情報を表示します。

例

#すべてのサービステンプレートに関する簡潔な情報を表示します。

[AP] display wlan service-template

```
Total number of service templates: 2
Service template name         SSID              Status
1                          2333              Enabled
2                          3222              Enabled
```

すべてのサービステンプレートに関する詳細な情報を表示します。

<AP> display wlan service-template verbose

```
Service template name        : service1
Description                  : Not configured
SSID                         : wuxianfuwu
SSID-hide                    : Disabled
User-isolation               : Disabled
Service template status      : Disabled
Maximum clients per BSS      : 64
VLAN ID                      : 1
AKM mode                     : PSK
Security IE                  : RSN
Cipher suite                 : CCMP
```

```
TKIP countermeasure time     : 100 sec
PTK lifetime                : 43200 sec
GTK rekey                   : Enabled
GTK rekey method             : Time-based
GTK rekey time              : 86400 sec
GTK rekey client-offline     : Enabled
User authentication mode     : Bypass
Intrusion protection         : Disabled
Intrusion protection mode    : Temporary-block
Temporary block time         : 180 sec
Temporary service stop time   : 20 sec
Fail VLAN ID                : 1
802.1X handshake             : Enabled
802.1X handshake secure      : Disabled
802.1X domain               : my-domain
MAC-auth domain             : Not configured
Max 802.1X users per BSS     : 4096
Max MAC-auth users per BSS   : 4096
802.1X re-authenticate       : Enabled
Authorization fail mode      : Online
Accounting fail mode         : Online
Authorization               : Permitted
Key derivation              : SHA1
PMF status                  : Optional
Hotspot policy number        : Not configured
Forwarding policy status     : Disabled
Forward policy name          : Not configured
Forwarder                   : AC
FT status                   : Enabled
QoS trust                   : Port
QoS priority                : 0
```

表 1-13 コマンド出力

フィールド	説明
SSID	サービステンプレートのSSID
SSID-hide	ひで • Disabled. • Enabled.
User-isolation	ユーザ分離 • Disabled. • Enabled.

フィールド	説明
Service template status	サービステンプレート status ● Disabled. ● Enabled.
Maximum clients per BSS	BSSがサポートするクライアントの最大数。
VLAN ID	クライアントがサービステンプレートを使用してオンラインになった後に属するVLANのID。
AKM mode	AKMモード ● 802.1X. ● PSK.
Security IE	Security IE ● RSN. ● WPA.
Cipher suite	暗号方式 ● WEP40. ● WEP104. ● WEP128. ● TKIP. ● CCMP.
TKIP countermeasure time	TKIP対策時間。設定値0は、対策が取られていないことを表します。
GTK rekey	GTK rekeyが有効/無効： ● Enabled. ● Disabled.
GTK rekey method	GTK rekey方式 ● 時間ベース ● パケットベース
GTK rekey time	GTK rekey間隔
GTK rekey packets	GTKをリフレッシュする前に送信できるパケット数。
GTK rekey client-offline	client-off GTK rekeyが有効/無効： ● Enabled. ● Disabled.

フィールド	説明
User authentication mode	認証モード ● **Bypass**–認証なし。 ● **MAC**. ● **MAC-or-802.1X**.－MAC認証が最初に実行されます。MAC認証に失敗すると、802.1X認証が実行されます。 ● **802.1X**. ● **802.1X-or-MAC**.－802.1X認証が最初に実行されます。802.1X認証に失敗するとMAC認証が実行されます。 ● **OUI-or-802.1X**.－OUI認証が最初に実行されます。OUI認証に失敗すると、802.1X認証を実行します。
Intrusion protection	侵入保護が有効/無効： ● Enabled. ● Disabled.
Intrusion protection mode	侵入防止モード： ● **Temporary-block**－ブロックリストに侵入者を一時的に追加します。 ● **Service-stop**－リセットされるまで、不正なパケットを受信するBSSによって提供されるすべてのサービスを停止します。 ● **Temporary-service-stop**－不正なパケットを受信したBSSが提供するアクセスサービスを一時的に停止します。
Temporary block time	一時的なブロック時間（秒）。
Temporary service stop time	一時的なサービス停止時間（秒）。
Fail VLAN ID	認証サーバが正常で認証に合格できない場合に、クライアントが追加されるVLANのID。未設定の場合“**Not configured**”が表示されます。
Critical VLAN ID	認証サーバが異常で認証に合格できない場合に、クライアントが追加されるVLANのID。未設定の場合“**Not configured**”が表示されます。
802.1X handshake	802.1Xハンドシェークが有効/無効： ● Enabled. ● Disabled.
802.1X handshake secure	セキュア802.1Xハンドシェークが有効/無効： ● Enabled. ● Disabled.
802.1X domain	802.1X認証ドメイン。未設定の場合“**Not configured**”が表示されます。

フィールド	説明
MAC-auth domain	MAC認証ドメイン。未設定の場合“**Not configured**”が表示されます。
Max 802.1X users per BSS	BSSでサポートされている802.1Xユーザの最大数
Max MAC-auth users per BSS	BSSでMAC認証に合格する、サポートされたユーザの最大数。
802.1X re-authenticate	802.1X再認証が有効/無効： ● Enabled. ● Disabled.
Authorization fail mode	許可失敗モード ● **Offline**－認証に失敗すると、クライアントはログオフされます。 ● **Online**－認証に失敗しても、クライアントはログオフされません。
Accounting fail mode	アカウンティング失敗モード ● **Offline**－アカウンティングに失敗すると、クライアントはログオフされます。 ● **Online**－アカウンティングに失敗しても、クライアントはログオフされません。
Authorization	許可情報： ● **Permitted**－RADIUSサーバまたはローカルデバイスによって発行された認可情報を適用します。 ● **Ignored**－RADIUSサーバまたはローカルデバイスによって発行された認証情報を無視します。
Key derivation	キーの導出タイプ ● **SHA1**－HMAC-SHA1 ハッシュアルゴリズム使用 ● **SHA256**－HMAC-SHA256 ハッシュアルゴリズム使用 ● **SHA1-AND-SHA256**－HMAC SHA1 and SHA256 ハッシュアルゴリズム使用
PMF status	PMFの状態 ● **Disabled**－管理フレームの保護が無効になっています。 ● **Optional**－オプションモードでの管理フレーム保護が有効になっています。 ● **Mandatory**－必須モードの管理フレーム保護が有効になっています。
Forwarding policy status	WLAN転送ポリシー状況 ● Disabled ● Enabled

フィールド	説明
Forward policy name	WLANフォワーディングポリシー ● **Not configured**－設定なし ● ポリシー名
Forwarder	クライアントトラフィックフォワーダ
FT status	FTの状態 ● Disabled. ● Enabled.
QoS trust	QoSプライオリティトラストモード： ● **Port**－Portプライオリティトラストモード ● **Dot11e**－802.11e プライオリティトラストモード
QoS priority	ポートプライオリティ。設定範囲は0～7です。

1.1.20 display wlan statistics client

Syntax

display wlan statistics client [**mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントを MAC アドレスで指定します。このオプションを指定しない場合、すべてのクライアントの統計が表示されます。

説明

display wlan statistics コマンドはクライアントの統計情報の統計情報を表示します。

例

すべてのクライアントの統計情報を表示します。

<AP> display wlan statistics client

```
MAC address              : 0014-6c8a-43ff
AP name                 : ap1
Radio ID                : 1
SSID                   : office
BSSID                  : 000f-e2ff-7700
RSSI                   : 31
Sent frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 9/1230 (frames/bytes)
  Video                : 0/0 (frames/bytes)
  Voice                : 2/76 (frames/bytes)
Received frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 18/2437 (frames/bytes)
  Video                : 0/0 (frames/bytes)
  Voice                : 7/468 (frames/bytes)
Discarded frames:
  Back ground           : 0/0 (frames/bytes)
  Best effort           : 0/0 (frames/bytes)
  Video                : 0/0 (frames/bytes)
```

```
  Voice                : 5/389 (frames/bytes)
```

表 1-14 コマンド出力

フィールド	説明
SSID	サービステンプレートのSSID
MAC address	クライアントのMACアドレス
Back ground	AC-BK queue.
Best effort	AC-BE queue.
Video	AC-VI queue.
Voice	AC-VO queue.

サービステンプレート 1 の統計情報を表示します。

<AP> display wlan statistics service-template 1

```
AP name                    : ap1
Radio ID                   : 1
Received:
  Frame count              : 1713
  Frame bytes              : 487061
  Data frame count          : 1683
  Data frame bytes          : 485761
  Association request count   : 2
Sent:
  Frame count              : 62113
  Frame bytes              : 25142076
  Data frame count          : 55978
  Data frame bytes          : 22626600
  Association response count  : 2
```

サービステンプレート 1 の接続履歴を表示します。

<AP> display wlan statistics service-template 1 connect-history

```
AP name                  : ap1
Radio ID                 : 1
Associations              : 132
Association failures       : 3
Reassociations            : 30
Rejections               : 12
Abnormal disassociations    : 2
Current associations       : 57
```

```
AP name                 : ap1
Radio ID                : 2
Associations             : 1004
Association failures       : 35
Reassociations            : 59
Rejections              : 4
Abnormal disassociations    : 22
Current associations       : 300
```

1.1.21 display wlan statistics connect-history

Syntax

display wlan statistics connect-history service-template *service-template-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template *service-template-name*: サービステンプレート名で指定します。

説明

display wlan statistics connect-history service-template コマンドはクライアントの接続履歴が表示します。

例

#サービステンプレート 1 の接続履歴を表示します。

<AP> display wlan statistics connect-history service-template 1

```
AP name                   : fatap
Radio ID                  : 1
Associations              : 132
Association failures      : 3
Reassociations            : 30
Rejections                : 12
Abnormal disassociations  : 2
Current associations      : 57
```

1.1.22 display wlan statistics service template

Syntax

display wlan statistics service-template *service-template-name*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

service-template *service-template-name*: サービステンプレート名で指定します。

説明

display wlan statistics service-template コマンドは、サービステンプレートの統計情報を表示します。

例

#サービステンプレート 1 の統計情報を表示します。

<AP> display wlan statistics connect-history service-template 1

```
AP name                       : fatap
Radio ID                      : 1
Received:
Frame count                   : 1713
 Frame bytes                  : 487061
 Data frame count             : 1683
Data frame bytes              : 485761
Association request count     : 2
Sent:
Frame count                   : 62113
 Frame bytes                  : 25142076
 Data frame count             : 55978
 Data frame bytes             : 22626600
Association response count    : 2
```

1.1.23 display wlan whitelist

Syntax

display wlan whitelist

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan whitelist コマンドはホワイトリストエントリを表示します。

例

#ホワイトリストエントリを表示します。

<AP> display wlan whitelist

```
Total number of clients: 3
 MAC addresses:
  000e-35b2-000e
  0019-5b8e-b709
  001c-f0bf-9c92
```

1.1.24 interface wlan-radio

Syntax

interface wlan-radio *interface-number*

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: インタフェースの番号を指定します。

説明

interface wlan-radio コマンドは radio interface view に移行します。

例

無線インタフェース WLAN-Radio 1/0/1 の view に移行します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1]

1.1.25 nas-id

Syntax

nas-id *nas-id*

undo nas-id

デフォルト

設定なし

View

Global configuration view

定義済みユーザロール

network-admin

パラメータ

nas-id: NAS ID を指定します。NAS ID は、1～63 文字の文字列です。大文字と小文字を区別します。

説明

nas-id コマンドは NAS ID（Network Access Server IDentifier）を設定します。

オンライン後、クライアントは、NAS ID を持つ RADIUS 要求を RADIUS サーバに送信して、ネットワークアクセスサーバを指定します。

サービステンプレートを無線にバインドするときに NAS ID を設定します。サービステンプレートを無線にバインドするときに NAS ID を指定した場合、AP はサービステンプレートに指定された NAS ID を使用します。

例

NAS ID abc123 を設定します。

<AP> system-view

[AP] wlan global-configuration

[AP-wlan-global-configuration] nas-id abc123

1.1.26 nas-port-type

Syntax

nas-port-type *value*

undo nas-port-type

デフォルト

IEEE 802.11

View

Service template view

定義済みユーザロール

network-admin

パラメータ

value: 0~255 の範囲のコード値で NAS ポートタイプを指定します。表 1-17 に、最も一般的に使用される NAS ポートタイプとそのコード値を示します。

表 1-15 コマンド出力

NAS ポートタイプ	コード値
Async	0
Sync	1
ISDN Sync	2
ISDN Async V.120	3
ISDN Async V.110	4
Virtual	5
PIAFS	6
HDLC Clear Channel	7
X.25	8
X.75	9
G.3 Fax	10
SDSL	11

NAS ポートタイプ	コード値
ADSL-CAP	12
ADSL-DMT	13
IDSL	14
Ethernet	15
xDSL	16
Cable	17
Wireless-Other	18
Wireless-IEEE 802.11	19

説明

nas-port-type コマンドは、RADIUS 要求に NAS ポートタイプ属性を設定します。

undo nas-port-type コマンドは、デフォルトに戻します。

このコマンドを実行して、802.11 X および MAC 認証クライアントの RADIUS 要求に NAS ポートタイプ属性を設定できます。

このコマンドを実行する前に、サービステンプレートが無効になっていることを確認してください。

例

RADIUS 要求の NAS ポートタイプを 15 (イーサネット) に設定します。

<AP> system-view

[AP] wlan service-template 1

[AP-wlan-st-1] nas-port-type 15

1.1.27 quick-association enable

Syntax

quick-association enable

undo quick-association enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

quick-association enable コマンドはクイックアソシエーションを有効にします。

undo quick-association enable コマンドはクイックアソシエーションを無効にします。

このコマンドは、AP が指定されたサービステンプレートに関連付けられたクライアント上でロードバランシングまたはバンドナビゲーションを実行できないようにします。

例

サービステンプレート 1 の quick association を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1]quick-association enable

1.1.28 reset wlan client

Syntax

reset wlan client { **all** | **mac-address** *mac-address* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべてのクライアントを指定します。

mac-address *mac-address*: MAC アドレスでクライアントを指定します。

説明

reset wlan client コマンドはクライアントをログオフします。

例

#すべてのクライアントをログオフします。

<AP> reset wlan client all

関連コマンド

display wlan client

1.1.29 reset wlan dynamic-blacklist

Syntax

reset wlan dynamic-blacklist [**mac-address** *mac-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: MAC アドレスでクライアントを指定します。このオプションを指定しないと、このコマンドはダイナミックブラックリストからすべてのクライアントを削除します。

説明

reset wlan dynamic-blacklist コマンドはクライアントをダイナミックブラックリストから削除します。

例

ダイナミックブラックリストからすべてのクライアントを削除します。

<AP> reset wlan dynamic-blacklist

ダイナミックブラックリストから指定したクライアントを削除します。

<AP> reset wlan dynamic-blacklist mac-address b8ca-32a2-df69

関連コマンド

display wlan blacklist

1.1.30 reset wlan statistics client

Syntax

reset wlan statistics client { **all** | **mac-address** *mac-address* }

View

User view

定義済みユーザロール

network-admin

パラメータ

all: すべてのクライアントを指定します。

mac-address *mac-address*: MAC アドレスでクライアントを指定します。

説明

reset wlan statistics client コマンドはクライアント統計情報を削除します。

例

すべてのクライアント統計情報を削除します。

<AP> reset wlan statistics client all

関連コマンド

display wlan statistics

1.1.31 reset wlan statistics service-template

Syntax

reset wlan statistics service-template *service-template-name*

View

User view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を、大文字と小文字を区別しない 1~63 文字の文字列で指定します。

説明

reset wlan statistics service-template コマンドは、サービステンプレートの統計情報を削除します。

例

サービステンプレート service 1 に関する統計情報をクリアします。

<AP> reset wlan statistics service-template service1

関連コマンド

display wlan statistics

1.1.32 service-template

Syntax

service-template *service-template-name*

undo service-template *service-template-name*

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

説明

service-template コマンドはサービステンプレートを無線もしくは無線インタフェースにバインドします。

undo service-template コマンドはサービステンプレートを無線もしくは無線インタフェースへのバインドを解除します。

例

サービステンプレート service1 をインタフェース WLAN-Radio 1/0/1 にバインドします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1] service-template service1

1.1.33 service-template enable

Syntax

service-template enable

undo service-template enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

service-template enable コマンドはサービステンプレートを有効にします。

undo service-template enable コマンドはサービステンプレートを無効にします。

AC 上の BSS（basic service set）の数が制限を超える場合、新しいサービステンプレートを有効にできません。

例

サービステンプレート service1 を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] service-template enable

1.1.34 snmp-agent trap enable wlan client

Syntax

snmp-agent trap enable wlan client

undo snmp-agent trap enable wlan client

デフォルト

クライアントアクセスのための SNMP 通知は、無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan client を使用して、クライアント アクセスの SNMP 通知を有効にします。

undo snmp-agent trap enable wlan client を使用して、クライアント アクセスの SNMP 通知を無効にします。

この機能を有効にすると、クライアントのステータスが変化するたびに、デバイスはクライアント ステータス変化通知を NMS に送信します。

例

クライアント アクセスの SNMP 通知を有効にします。

```
<AP> system-view
[AP] snmp-agent trap enable wlan client
```

-
-
-

1.1.35 ssid

Syntax

ssid *ssid-name*

undo ssid

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID 名を 1～32 文字の文字列で指定します。SSID 名には、大文字、小文字、数字、特殊文字が使用可能です。大文字と小文字は区別されます。特殊文字については 表 1-16 を参照してください。

表 1-16 使用可能な特殊文字

名称	文字	名称	文字
Tilde	~	Left angle bracket	<
Exclamation point	!	Right angle bracket	>
At sign	@	Hyphen	-
Pound sign	#	Underscore	_
Dollar sign	$	Plus sign	+
Percent sign	%	Equal sign	=
Caret	^	Vertical bar	|
Ampersand sign	&	Backslash	¥
Asterisk	*	Colon	:
Left brace	{	Semi-colon	;
Right brace	}	Quotation marks	"

名称	文字	名称	文字
Left parenthesis	(	Apostrophe	'
Right parenthesis	)	Comma	,
Left bracket	[	Dot	.
Right bracket	]	Slash	/

説明

ssid コマンドはサービステンプレートに SSID を設定します。

undo ssid コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートを無効にしてください。

例

サービステンプレート service1 に SSID lynn を設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] ssid lynn

1.1.36 unknown-client

Syntax

unknown-client { **deauthenticate** | **drop** }

undo unknown-client

デフォルト

AP は未知のクライアントからのパケットを廃棄し、未知のクライアントの認証を解除します。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

deauthenticate: 未知のクライアントからのパケットを廃棄し、未知のクライアントの認証を解除します。

drop: 未知のクライアントからのパケットを廃棄します。

説明

unknown-client コマンドは未知のクライアントからのトラフィックを AP が処理する方法を設定します。

undo unknown-client コマンドはデフォルトに戻します。

例

未知のクライアントからのパケットを廃棄するが、未知のクライアントの認証は解除しないように AP を設定します。

<AP> system-view

[AP] wlan service-template example

[AP -wlan-st-example] unknown-client drop

1.1.37 vip limit rate

Syntax

vip limit rate level *level* { **inbound** | **outbound** } **mode** { **dynamic** [**min** *min-cir*] [**max** *max-cir*] | **static** } **cir** *cir*

undo vip limit rate level *level* { **inbound** | **outbound** }

デフォルト

無効

View

VIP client group view

定義済みユーザロール

network-admin

パラメータ

level *level*: VIP クライアントのレベルを指定します。2 つのみ使用できます。

inbound: 着信トラフィックのレートを制限します。

vlan-id: VLAN を VLAN ID で指定します。VLAN ID の設定範囲は 1〜4094 です。

dynamic: ダイナミックレート制限モードを指定します。このモードでは、各クライアントの制限レートは、CIR の合計をクライアント数で割った値になります。

min *min-cir*: 各クライアントの最小 CIR を 16~1700000Kbps の範囲で指定します。このオプションを指定しない場合、コマンドは最小合計 CIR を制限しません。

max *max-cir*: クライアントごとの最大 CIR を 16~1700000Kbps の範囲で指定します。最大 CIR は最小 CIR より大きくする必要があります。このオプションを指定しない場合、コマンドは最大合計 CIR を制限しません。

static: スタティックレート制限モードを指定します。このモードでは、各クライアントの制限レートは固定値です。

cir *cir*: CIR を Kbps 単位で指定します。cir 引数の値の範囲は 16~1700000Kbps です。

説明

vip limit rate コマンドは、VIP クライアントのレート制限を有効にします。

undo vip limit rate コマンドは、デフォルトに戻します。

多数の VIP クライアントがオンラインになっている場合は、このタスクを実行して VIP クライアントのレートを制限し、各クライアントの帯域幅を保証して良好なユーザーエクスペリエンスを確保できます。

ダイナミックレート制限に最小 CIR と最大 CIR の両方を指定した場合、この機能は次のように動作します。

- 指定した CIR をクライアントの総数で割った値が最小 CIR より小さい場合、最小 CIR はクライアントごとに有効になります。
- 指定した CIR をクライアントの総数で割った値が最大 CIR より大きい場合、最大 CIR はクライアントごとに有効になります。
- 指定した CIR をクライアントの総数で割った値が最小 CIR と最大 CIR の間にある場合、指定した CIR をクライアントの総数で割った値がクライアントごとに有効になります。

このコマンドを複数回実行して、着信トラフィックと発信トラフィックの両方のレートを制限できます。

VIP クライアントのレート制限と無線ベースのクライアントのレート制限の両方を設定した場合、有効になる設定はレート制限モード (スタティックまたはダイナミック) によって異なります。

- 異なるレート制限モードが設定されている場合、VIP クライアントのレート制限が有効になります。
- スタティックモードが設定されている場合、より小さい CIR が有効になります。
- ダイナミックモードが設定されている場合、VIP クライアントのレート制限が有効になります。

例

U スタティック VIP クライアントのレート制限を設定します:着信トラフィックの CIR を 500 Kbps に設定し、発信トラフィックの CIR を 100 Kbps に設定します。

<AP> system-view

[AP] wlan vip-client-group

[AP-vip-client-group] vip limit rate level 2 inbound mode static cir 500

[AP-vip-client-group] vip limit rate level 2 outbound mode static cir 100

関連コマンド

- **client-rate-limit** (無線ビュー/AP グループ無線ビュー)

1.1.38 vlan

Syntax

vlan *vlan-id*

undo vlan

デフォルト

サービステンプレートに VLAN 1 がバインドされています。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

vlan-id: VLAN を VLAN ID で指定します。VLAN ID の設定範囲は 1～4094 です。

説明

vlan コマンドはサービステンプレートを使用してオンラインになったクライアントに特定の VLAN を割り当てます。

undo vlan コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートを無効にしてください。

指定した VLAN が存在しない場合、このコマンドは、クライアントがオンラインになったときに VLAN を作成します。

例

サービステンプレート service1 を使用してオンラインになったクライアントを VLAN 2 に割り当てます。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] vlan 2

1.1.39 wlan association optimization

Syntax

wlan association optimization *value*

undo association optimization

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

value: クライアントアソシエーション比を最適化するためのインデックスを 900~1000 の範囲で指定します。インデックスが小さいほど、計算されたアソシエーション成功率は小さくなり、計算された輻輳比と異常なアソシエーション比は大きくなります。

説明

wlan association optimization コマンドは、クライアントアソシエーション比を最適化するためのインデックスを設定します。

undo wlan association optimization コマンドは、デフォルトに戻します。

この機能を使用すると、装置は指定されたインデックスを使用してクライアントアソシエーション成功率、アソシエーション輻輳率、および異常なアソシエーション切断率を再計算し、より小さい比率値を取得できます。

クライアントアソシエーションの成功率は、成功したクライアントアソシエーションの数をクライアントアソシエーションの試行の合計数で割った値です。クライアントアソシエーションの輻輳率は、AP の過負荷によって発生した失敗したクライアントアソシエーションの数をクライアントアソシエーションの試行の合計数で割った値です。クライアントの異常なアソシエーションの割合は、異常なアソシエーションの数を成功したアソシエーションとオンラインクライアントの合計で割った値です。

例

クライアントアソシエーション比を最適化するためのインデックスを 950 に設定します。

<AP> system-view

[AP] wlan association optimization 950

1.1.40 wlan broadcast-probe reply

Syntax

wlan broadcast-probe reply [rssi-threshold rssi-value **] [frequency-band**

{ 2.4 | 5 } **]**

undo wlan broadcast-probe reply [frequency-band { 2.4 | 5 **}]**

デフォルト

ブロードキャストプローブ要求に応答します。

View

System view

定義済みユーザロール

network-admin

パラメータ

rssi-threshold rssi-value: 1 ～ 100 の範囲で RSSI しきい値を指定します。このオプションを指定しない場合、このコマンドは、AP がすべての RSSI を使用してブロードキャストプローブ要求に応答できるようにします。

frequency-band: 周波数帯域を指定します。このキーワードを指定しない場合、このコマンドにより、AP は 5 GHz と 2.4 GHz の両方の帯域で受信したブロードキャストプローブ要求に応答できるようになります。

2.4: 2.4 GHz 帯域を指定します。

5: 5 GHz 帯域を指定します。

説明

wlan broadcast-probe reply コマンドは AP がブロードキャストプローブ要求に応答できるようにします。

undo wlan broadcast-probe reply コマンドは AP がブロードキャストプローブ要求に応答できなくします。(SSID が空欄である場合の ANY 接続拒否)

🕮 **メモ**:

SSID が“ANY”の文字列である ANY 接続は、本コマンドの有効無効に限らず“ANY”の文字列を持つサービステンプレートを作成しなければ接続されません。

例

AP がブロードキャストプローブ要求に応答できないように設定します。

<AP> system-view

[AP] undo wlan broadcast-probe reply

1.1.41 wlan client bss-load-ie enable

Syntax

wlan client bss-load-ie enable [**update-interval** *interval*]

undo client bss-load-ie enable

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

update-interval *interval*: BSS Load IE の更新間隔を 5~30 秒の範囲で指定します。デフォルト値は 15 です。

説明

wlan client bss-load-ie enable コマンドは、ビーコンフレームとプローブ応答で BSS Load IE を伝送できるようにします。

undo wlan client bss-load-ie enable コマンドは、デフォルトに戻します。

この機能を有効にすると、装置によって送信されるビーコンフレームとプローブ応答は BSS Load IE を伝送します。IE には、無線上の各 BSS のクライアント数、チャネル使用率、および残りのメディア時間が含まれます。

ローミングネットワークでは、クライアントが BSS Load IE を使用して最適なネットワークを選択するための最善策として、この機能を有効にします。

例

ビーコンフレームとプローブ応答を有効にして、BSS Load IE を伝送します。

<AP> system-view

[AP] wlan client bss-load-ie enable

1.1.42 wlan client failure history aging

Syntax

wlan client failure history aging *aging-time*

undo wlan client failure history aging

デフォルト

システムは、クライアント アソシエーションの失敗を最大 72 時間保存できます。

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: クライアント アソシエーション失敗レコードのエージング タイマーを 1 ～ 720 時間の範囲で指定します。

説明

wlan client failure history aging を使用して、クライアント アソシエーション障害レコードのエージング タイマーを指定します。

undo wlan client failure history aging を使用してデフォルトに戻します。

デバイスは、最大 512 個のクライアント アソシエーション失敗レコードを保存できます。

レコード数がこの上限を超えると、システムは最も古いレコードを自動的に削除します。

レコード数がこの上限を超えていなくても、このコマンドで指定したエージング タイマーがタイムアウトした場合、システムは期限切れのレコードを削除します。

例

クライアント アソシエーションの失敗に対するエージング タイマーを 700 時間に設定します。

```
<AP> system-view
[AP] wlan client failure history aging 700
```

-
-

1.1.43 wlan client idle-timeout

Syntax

wlan client idle-timeout *timeout*

undo wlan client idle-timeout

デフォルト

v7.5.98 と v7.5.105：

3600 (秒) (コンフィグ上では非表示)

V7.5.114 以降：

300 (秒) (コンフィグ上では非表示)

View

System view

定義済みユーザロール

network-admin

パラメータ

timeout: クライアントアイドルタイムアウト時間を指定します。設定範囲は 60～86400 秒です。

説明

wlan client idle-timeout コマンドはクライアントアイドルタイムアウトタイマを設定します。

undo wlan client idle-timeout コマンドはデフォルト設定に戻します。

クライアントが AP に接続しているとき、クライアントアイドルタイムアウト時間内に、接続した AP に対してクライアントがフレームを送信しない場合、AP はクライアントをログオフします。

例

クライアントアイドルタイムアウト時間を 2000 秒に設定します。

<AP> system-view

[AP] wlan client idle-timeout 2000

1.1.44 wlan client keep-alive

Syntax

wlan client keep-alive enable

undo wlan client keep-alive

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

wlan client keep-alive enable コマンドはクライアントキープアライブを有効にします。

undo wlan client keep-alive コマンドはクライアントキープアライブを無効にします。

この機能を有効にすることで、AP はクライアントがオンラインであるか判断するため、指定された間隔でクライアントに対してキープアライブパケットを送信できるようになります。クライアントからの応答が 3 キープアライブ間隔以内にない場合、AP はクライアントをログオフします。

例

クライアントキープアライブを有効にします。

<AP> system-view

[AP] wlan client keep-alive enable

関連コマンド

wlan client keep-alive interval

1.1.45 wlan client keep-alive interval

Syntax

wlan client keep-alive interval *interval*

undo wlan client keep-alive interval

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: クライアントのキープアライブ間隔を指定します。設定範囲は 3～1800 秒です。

説明

wlan client keep-alive interval コマンドはクライアントのキープアライブ間隔を設定します。

undo wlan client keep-alive interval コマンドはデフォルトに戻します。

このコマンドを使用する前に、クライアントキープアライブを AP で有効にしてください。

この機能を有効にすることで、AP はクライアントがオンラインであるか判断するため、指定された間隔でクライアントに対してキープアライブパケットを送信できるようになります。クライアントからの応答が 3 キープアライブ間隔以内にない場合、AP はクライアントをログオフします。

例

クライアントキープアライブ間隔を 1000 秒に設定します。

<AP> system-view

[AP] wlan client keep-alive interval 1000

関連コマンド

wlan client keep-alive

1.1.46 wlan client reauthentication-period

Syntax

wlan client reauthentication-period [*period-value*]

undo wlan client reauthentication-period

デフォルト

10 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

period-value: アイドル期間を指定します。設定範囲は 1～3600 秒です。デフォルトでは、アイドル期間は 10 秒です。

説明

wlan client reauthentication-period コマンドはクライアント再認証の前にアイドル期間を設定します。

undo wlan client reauthentication-period コマンドはデフォルトに戻します。

再認証の失敗を減らすためにクライアント再認証のまえにアイドル期間を設定します。

URL リダイレクトが WLAN MAC 認証クライアントに対して有効なとき、AP は MAC 認証をパスしたクライアントをログオフします。次回 MAC 認証を行う際、クライアントは MAC 認証をパスし WLAN にアクセスできます。アイドル期間を設定すると、AP はクライアントをログオフした後にそのクライアントをブラックリストに追加します。指定したアイドル期間経過後、クライアントエントリはエージアウトします。

例

クライアント再認証のまえにアイドル期間を 100 秒に設定します。

<AP> system-view

[AP] wlan client reauthentication-period 100

1.1.47 wlan dynamic-blacklist lifetime

Syntax

wlan dynamic-blacklist lifetime *lifetime*

undo wlan dynamic-blacklist lifetime

デフォルト

300 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

lifetime: エージングタイムを指定します。設定範囲は 1～3600 秒です。

説明

wlan dynamic-blacklist lifetime コマンドはダイナミックブラックリストエントリにエージングタイムを設定します。

undo wlan dynamic-blacklist lifetime コマンドはデフォルトに戻します。

設定したエージングタイムは、設定後、ダイナミックブラックリストに追加されたエントリから有効です。

ダイナミックブラックリストエントリのエージングタイムは不正なクライアントエントリにのみ適用されます。

例

ダイナミックブラックリストのエージングタイムを 3600 秒に指定します。

<AP> system-view

[AP] wlan dynamic-blacklist lifetime 3600

1.1.48 wlan link-test

Syntax

wlan link-test *mac-address*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

mac-address: H-H-H 形式でクライアント MAC アドレスを指定します。

説明

wlan link-test コマンドは無線リンク品質をテストします。

無線リンク品質検出により、AP は無線クライアントへのリンクの品質をテストできます。AP は、各サポートレートでクライアントに空のデータフレームを送信します。次に、クライアントからの応答に基づいて、RSSI、パケット再送信、RTT などのリンク品質情報を計算します。

無線リンク品質検出のタイムアウト時間は 10 秒です。タイムアウト時間内で無線リンク検出が完了しない場合、テスト結果を取得できません。

例

MAC アドレス 60a4-4cda-eff0 のクライアントに対して、無線リンク品質検出を実行します。

<AP> wlan link-test 60a4-4cda-eff0

```
Testing link to 60a4-4cda-eff0. Press CTRL + C to break.
                        Link Status
--------------------------------------------------------------------------
MAC address: 60a4-4cda-eff0
--------------------------------------------------------------------------
VHT-MCS  Rate(Mbps)  TxCnt      RxCnt      RSSI  Retries  RTT(ms)
--------------------------------------------------------------------------
NSS = 1
--------------------------------------------------------------------------
 0      32.5        5          5          54    0        0
 1      65          5          5          51    0        0
 2      97.5        5          5          49    0        0
 3      130         5          5          47    0        0
 4      195         5          5          45    0        0
 5      260         5          5          45    0        0
```

```
 6       292.5       5           5           44      0       0
 7       325         5           5           44      0       0
 8       390         5           5           44      0       0
 9       433.3       5           5           43      0       0
------------------------------------------------------------------------
NSS = 2
------------------------------------------------------------------------
 0       65          5           5           44      0       0
 1       130         5           5           44      0       0
 2       195         5           5           44      0       0
 3       260         5           5           44      0       0
 4       390         5           5           44      0       0
 5       520         5           5           44      0       0
 6       585         5           5           43      0       0
 7       650         5           5           43      0       0
 8       780         5           5           43      0       0
 9       866.7       5           5           43      0       0
```

表 1-17 コマンド出力

フィールド	説明
No./MCS/VHT-MCS/HE-MCS	• **No**－802.11a、802.11b、802.11gクライアントのリンク品質テストの速度番号。 • **MCS**－802.11nクライアントのリンク品質テストのMCSインデックス。 • **VHT-MCS**－802.11acクライアントのリンク品質テストのVHT-MCSインデックス。 • **HE-MCS**－802.11axクライアントのリンク品質テストのHE-MCSインデックス。
Rate(Mbps)	APが無線リンク品質検出フレームを送信するレート。
TxCnt	APが送信した無線リンク品質検出フレームの数。
RxCnt	APが受信した応答数。
RSSI	APが検出したクライアントのRSSI。
Retries	無線リンク品質検出フレームの再送信の数。
RTT(ms)	APからクライアントへの無線リンク品質検出フレームのラウンドトリップ時間。
NSS	802.11nまたは802.11ac/axクライアントでのリンク品質テスト用の空間ストリームの数。

1.1.49 wlan nas-port-id format

Syntax

wlan nas-port-id format { **2** | **4** }

undo wlan nas-port-id format

デフォルト

クライアントは形式 2 を使用して NAS ポート ID を生成します。

View

System view

定義済みユーザロール

network-admin

パラメータ

2: **SlotID 00 IfNOVlanID** 形式を指定します。

- SlotID –クライアントアクセス用のスロット ID、2 文字の文字列。
- IfNO –クライアントアクセスのインターフェース番号、3 文字の文字列。
- VlanID – クライアントアクセス用の VLAN ID、9 文字の文字列。

4: **slot=**;subslot=**;port=**;vlanid=**;vlanid2=**形式で指定します。**vlanid 2** フィールドは VLAN ターミネーションが設定されたインタフェースを介して WLAN にアクセスするクライアントに対してのみ使用できます。

説明

wlan nas-port-id format コマンドは、無線クライアントの NAS ポート ID の形式を設定します。

undo wlan nas-port-id format コマンドは、デフォルトに戻します。

802.1 X および MAC 認証クライアントは、RADIUS パケットに指定された形式で NAS ポート ID を入力します。

例

NAS ポート ID の形式を形式 4 に設定します。

<AP> system-view

[AP] wlan nas-port-id format 4

1.1.50 wlan service-template

Syntax

wlan service-template *service-template-name*

undo wlan service-template *service-template-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

service-template-name: サービステンプレート名を指定します。サービステンプレート名は、1～63 文字の文字列です。大文字と小文字を区別しません。

説明

wlan service-template コマンドはサービステンプレートを作成し、その view に移行する、あるいは既存のサービステンプレートに移行します。

undo wlan service-template コマンドはサービステンプレートを削除します。

無線にバインドされているサービステンプレートは削除できません。

例

サービステンプレート service1 を作成し、その view に移行します。

<AP> system-view

[AP] wlan service-template service1

1.1.51 wlan static-blacklist mac-address

Syntax

wlan static-blacklist mac-address *mac-address*

undo wlan static-blacklist [**mac-address** *mac-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: MAC アドレスによりクライアントを指定します。形式は H-H-H です。undo コマンドで、このオプションを省略した場合、静的ブラックリストからすべてのクライアントを削除します。

説明

wlan static-blacklist mac-address コマンドはクライアントを静的ブラックリストに追加します。

undo wlan static-blacklist mac-address コマンドはクライアントを静的ブラックリストから削除します。

静的ブラックリストにオンラインクライアントを追加すると、クライアントをログオフします。

ホワイトリストと静的ブラックリストの両方にクライアントを追加することはできません。

例

静的ブラックリストに MAC アドレス 001c-f0bf-9c92 を追加します。

<AP> system-view

[AP] wlan static-blacklist mac-address 001c-f0bf-9c92

関連コマンド

display wlan blacklist

1.1.52 wlan web-server api-path

Syntax

wlan web-server api-path *path*

undo wlan web-server api-path

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

path: パス (大文字と小文字を区別する 1~256 文字の文字列) を指定します。

説明

wlan wlan web-server api-path コマンドは、クライアント情報を報告する Web サーバのパスを指定します。

undo wlan web-server api-path コマンドは、デフォルトに戻します。

Web サーバは、サーバのホスト名、ポート番号、およびパスが指定されている場合にのみクライアント情報を受け入れます。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

Web サーバのパスを**/wlan/dev-cfg** と指定します。

<AP> system-view

[AP] wlan web-server api-path /wlan/dev-cfg

関連コマンド

- **wlan web-server host**
- **wlan web-server max-client-entry**

1.1.53 wlan web-server host

Syntax

wlan web-server host *host-name* **port** *port-number*

undo web-server host

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

host *host-name*: ホスト名、大文字と小文字を区別しない 3~127 文字以内の文字列を指定します。文字、数字、ハイフン(-)、アンダースコア(_)、ドット (。) を使用できます。

port *port-number*: ポート番号を 1~65534 の範囲で指定します。

説明

wlan web-server host コマンドは、クライアント情報を通知する Web サーバのホスト名とポート番号を指定します。

undo wlan web-server host コマンドはクライアントをホワイトリストから削除します。

Web サーバは、サーバのホスト名、ポート番号、およびパスが指定されている場合にのみクライアント情報を受け入れます。

クライアント情報の変更は、リアルタイムで Web サーバに報告されます。

このコマンドを複数回実行すると、最新の設定が有効になります。

例

Web サーバのホスト名とポート番号をそれぞれ **www.abc.com, 668** と指定します。

<AP> system-view

[AP] wlan web-server host www.abc.com port 668

関連コマンド

- **wlan web-server api-path**
- **wlan web-server max-client-entry**

1.1.54 wlan web-server max-client-entry

Syntax

wlan web-server max-client-entry *number*

undo wlan web-server max-client-entry

デフォルト

一度に最大 10 のクライアントエントリを報告できます。

View

System view

定義済みユーザロール

network-admin

パラメータ

number: 一度に報告できるクライアントエントリの最大数を 1~25 の範囲で指定します。

説明

wlan web-server max-client-entry コマンドは一度に報告できるクライアントエントリの最大数を設定します。

undo web-server max-client-entry コマンドはデフォルトに戻します。

例

一度に報告できるクライアントエントリの最大数を 12 に設定します。

<AP> system-view

[AP] wlan web-server max-client-entry 12

関連コマンド

- **wlan web-server api-path**
- **wlan web-server host**

1.1.55 wlan whitelist mac-address

Syntax

wlan whitelist mac-address *mac-address*

undo wlan whitelist [**mac-address** *mac-address*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address *mac-address*: MAC アドレスによりクライアントを指定します。形式は H-H-H です。undo コマンドで、このオプションを省略した場合、ホワイトリストからすべてのクライアントを削除します。

説明

wlan whitelist mac-address コマンドはクライアントをホワイトリストに追加します。

undo wlan whitelist mac-address コマンドはクライアントをホワイトリストから削除します。

最初のクライアントをホワイトリストに追加すると、すべてのオンラインクライアントを切断するかどうかを尋ねるメッセージが表示されます。“Y”と入力するとホワイトリストが作成されます。ホワイトリストからオンラインクライアントを削除すると、クライアントをログオフします。ホワイトリストからすべてのクライアントを削除すると、オンラインクライアントはログオフされません。

ホワイトリストと静的ブラックリストの両方にクライアントを追加することはできません。

例

#ホワイトリストに MAC アドレス 0055-f0bf-9c92 を追加します。

<AP> system-view

[AP] wlan whitelist mac-address 0055-f0bf-9c92

```
This command will disconnect all clients. Continue? [Y/N]:
```

関連コマンド

display wlan whitelist

目次

このセクションのページは **7-x-x** です。

2 章 WIPS 2-1
2.1 WIPS の設定コマンド 2-1
2.1.1 access-scan 2-1
2.1.2 ap-channel-change 2-2
2.1.3 ap-classification rule 2-3
2.1.4 ap-flood 2-4
2.1.5 ap-impersonation 2-5
2.1.6 apply ap-classification rule 2-6
2.1.7 apply classification policy 2-7
2.1.8 apply countermeasure policy 2-8
2.1.9 apply detect policy 2-9
2.1.10 apply signature policy 2-10
2.1.11 apply signature rule 2-11
2.1.12 ap-rate-limit 2-12
2.1.13 ap-spoofing 2-13
2.1.14 ap-timer 2-14
2.1.15 association-table-overflow 2-15
2.1.16 authentication 2-16
2.1.17 block mac-address 2-17
2.1.18 classification policy 2-18
2.1.19 client-association fast-learn enable 2-19
2.1.20 client-online 2-20
2.1.21 client-rate-limit 2-21
2.1.22 client-spoofing 2-22
2.1.23 client-timer 2-23
2.1.24 countermeasure adhoc 2-24
2.1.25 countermeasure attack all 2-25
2.1.26 countermeasure attack deauth-broadcast 2-26
2.1.27 countermeasure attack disassoc-broadcast 2-27
2.1.28 countermeasure attack honeypot-ap 2-28
2.1.29 countermeasure attack hotspot-attack 2-29
2.1.30 countermeasure attack ht-40-mhz-intolerance 2-30
2.1.31 countermeasure attack malformed-packet 2-31
2.1.32 countermeasure attack man-in-the-middle 2-32
2.1.33 countermeasure attack omerta 2-33
2.1.34 countermeasure attack power-save 2-34

2.1.35 countermeasure attack soft-ap 2-35
2.1.36 countermeasure attack unencrypted-trust-client 2-36
2.1.37 countermeasure attack weak-iv 2-37
2.1.38 countermeasure attack windows-bridge 2-38
2.1.39 countermeasure enhance 2-39
2.1.40 countermeasure external-ap 2-40
2.1.41 countermeasure mac-address 2-41
2.1.42 countermeasure misassociation-client 2-42
2.1.43 countermeasure misconfigured-ap 2-43
2.1.44 countermeasure packet-sending-interval 2-44
2.1.45 countermeasure policy 2-45
2.1.46 countermeasure potential-authorized-ap 2-46
2.1.47 countermeasure potential-external-ap 2-47
2.1.48 countermeasure potential-rogue-ap 2-48
2.1.49 countermeasure rogue-ap 2-49
2.1.50 countermeasure unauthorized-client 2-50
2.1.51 countermeasure uncategorized-ap 2-51
2.1.52 countermeasure uncategorized-client 2-52
2.1.53 deauthentication-broadcast 2-53
2.1.54 deauth-spoofing 2-54
2.1.55 detect dissociate-client enable 2-55
2.1.56 detect policy 2-56
2.1.57 detect signature 2-57
2.1.58 disassociation-broadcast 2-58
2.1.59 discovered-ap 2-59
2.1.60 display wips sensor 2-60
2.1.61 display wips statistics 2-61
2.1.62 display wips virtual-security-domain countermeasure record 2-65
2.1.63 display wips virtual-security-domain device 2-67
2.1.64 embedded-oui-classify enable 2-73
2.1.65 export oui 2-74
2.1.66 flood association-request 2-75
2.1.67 flood authentication 2-76
2.1.68 flood beacon 2-77
2.1.69 flood block-ack 2-78
2.1.70 flood cts 2-79
2.1.71 flood deauthentication 2-80
2.1.72 flood disassociation 2-81
2.1.73 flood eap-failure 2-82
2.1.74 flood eapol-logoff 2-83
2.1.75 flood eapol-start 2-84
2.1.76 flood eap-success 2-85
2.1.77 flood null-data 2-86

2.1.78 flood probe-request 2-87
2.1.79 flood reassociation-request 2-88
2.1.80 flood rts 2-89
2.1.81 frame-type 2-90
2.1.82 honeypot-ap 2-91
2.1.83 hotspot-attack 2-92
2.1.84 hotspot ssid 2-93
2.1.85 ht-40mhz-intolerance 2-94
2.1.86 ht-greenfield 2-95
2.1.87 ignorelist 2-96
2.1.88 import hotspot 2-97
2.1.89 import oui 2-98
2.1.90 invalid-oui-classify illegal 2-99
2.1.91 mac-address 2-100
2.1.92 malformed duplicated-ie 2-101
2.1.93 malformed fata-jack 2-102
2.1.94 malformed illegal-ibss-ess 2-103
2.1.95 malformed invalid-address-combination 2-104
2.1.96 malformed invalid-assoc-req 2-105
2.1.97 malformed invalid-auth 2-106
2.1.98 malformed invalid-deauth-code 2-107
2.1.99 malformed invalid-disassoc-code 2-108
2.1.100 malformed invalid-ht-ie 2-109
2.1.101 malformed invalid-ie-length 2-110
2.1.102 malformed invalid-pkt-length 2-111
2.1.103 malformed large-duration 2-112
2.1.104 malformed null-probe-resp 2-113
2.1.105 malformed overflow-eapol-key 2-114
2.1.106 malformed overflow-ssid 2-115
2.1.107 malformed redundant-ie 2-116
2.1.108 man-in-the-middle 2-117
2.1.109 manual-classify mac-address 2-118
2.1.110 match all (AP classification rule view) 2-119
2.1.111 match all (signature view) 2-120
2.1.112 omerta 2-121
2.1.113 oui 2-122
2.1.114 pattern 2-123
2.1.115 permit-channel 2-125
2.1.116 power-save 2-126
2.1.117 prohibited-channel 2-128
2.1.118 random-mac-scan 2-129
2.1.119 report-interval 2-130
2.1.120 reset wips embedded-oui 2-131

2.1.121 reset wips statistics 2-132
2.1.122 reset wips virtual-security-domain 2-133
2.1.123 reset wips virtual-security-domain countermeasure record 2-134
2.1.124 rssi-change-threshold 2-135
2.1.125 rssi-threshold 2-136
2.1.126 rssi 2-137
2.1.127 security 2-138
2.1.128 select sensor all 2-139
2.1.129 seq-number 2-140
2.1.130 signature policy 2-141
2.1.131 signature rule 2-142
2.1.132 soft-ap 2-143
2.1.133 ssid (AP classification rule view) 2-144
2.1.134 ssid (signature view) 2-145
2.1.135 ssid-length 2-146
2.1.136 trust mac-address 2-147
2.1.137 trust oui 2-148
2.1.138 trust ssid 2-149
2.1.139 unencrypted-authorized-ap 2-150
2.1.140 unencrypted-trust-client 2-151
2.1.141 up-duration 2-152
2.1.142 virtual-security-domain 2-153
2.1.143 weak-iv 2-154
2.1.144 windows-bridge 2-155
2.1.145 wips(system view) 2-156
2.1.146 wips(radio view) 2-157
2.1.147 wips virtual-security-domain 2-158
2.1.148 wireless-bridge 2-159

2章 WIPS

🕮 **メモ：**

- WIPS の機能はソフトウェアバージョン 7.5.105 を含む以降のソフトウェアからサポートしています。

2.1 WIPSの設定コマンド

2.1.1 access-scan

Syntax

access-scan enable

undo access-scan enable

デフォルト

無効

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がチャネル変更のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にチャネル変更を検出してもアラームを引き起こしません。

説明

ap-channel-change コマンドはアクセスサービスを提供しながら、AP による WIPS スキャンの実行を無効します。

このコマンドは、WIPS の検出および保護機能を強化しますが、アクセスサービス機能を低下させます

例

アクセスサービスを提供しながら、WIPS スキャンを実行するように AP を設定します。

<AP> system-view

[AP] wips

[AP] access-scan enable

2.1.2 ap-channel-change

Syntax

ap-channel-change [**quiet** *quiet-value*]

undo ap-channel-change

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がチャネル変更のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にチャネル変更を検出してもアラームを引き起こしません。

説明

ap-channel-change コマンドはチャネル変更を設定します。

undo ap-channel-change コマンドはチャネル変更の検出を無効にします。

例

チャネル変更の検出を有効にし、遅延時間を 5 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-channel-change quiet 5

2.1.3 ap-classification rule

Syntax

ap-classification rule *rule-id*

undo ap-classification rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で AP 分類ルールを指定します。値の範囲は 1～65535 です。

説明

ap-classification rule コマンドは AP 分類ルールを作成し、その view に移行します。AP 分類ルールがすでに存在する場合、**ap-classification rule** コマンドで AP 分類ルール view に移行します。

undo ap-classification rule コマンドは AP 分類ルールを削除します。

例

AP classification rule 1 を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

2.1.4 ap-flood

Syntax

ap-flood [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *

undo ap-flood

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

apnum *apnum-value*: AP 数しきい値を指定します。値の範囲は 10～200 です。デフォルト値は 80 です。

exceed *exceed-value*: 超過を許可された AP の最大数を指定します。*exceed-value* 引数の値の範囲は 10～200 です。デフォルト値は 80 です。AP の数が、AP 数しきい値と、超過を許可された AP の最大数の合計を超える場合、WIPS は AP フラッド攻撃アラームを引き起こします。

quiet *quiet-value*: WIPS が AP フラッド攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP フラッド攻撃を検出してもアラームを引き起こしません。

説明

ap-flood コマンドは AP フラッド攻撃検出を設定します。

undo ap-flood コマンドは AP フラッド攻撃検出を無効にします。

例

AP フラッド攻撃検出を有効にし、*apnum-value*、*exceed-value*、*quiet-value* をそれぞれ 50、50、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-flood apnum 50 exceed 50 quiet 100

2.1.5 ap-impersonation

Syntax

ap-impersonation [**quiet** *quiet-value*]

undo ap-impersonation

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP なりすまし攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP なりすまし攻撃を検出してもアラームを引き起こしません。

説明

ap-impersonation コマンドは AP なりすまし攻撃検出を設定します。

undo ap-impersonation コマンドはデフォルトに戻します。

例

AP なりすまし攻撃検出を有効にし、遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-impersonation quiet 360

2.1.6 apply ap-classification rule

Syntax

apply ap-classification rule *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }

undo apply ap-classification rule *rule-id*

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で AP 分類ルールを指定します。ID の値の範囲は 1～65535 です。

authorized-ap: 許可された AP として AP 分類ルールに一致する AP を指定します。

external-ap: 外部 AP

misconfigured-ap: 不良コンフィグレーション AP として AP 分類ルールに一致する AP を指定します。

rogue-ap: 不正な AP として AP 分類ルールに一致する AP を指定します。

level: AP 分類ルールに一致する AP に対して重大度レベルを指定します。レベルの範囲は 1～100 です。デフォルトレベルは 50 です。

説明

apply ap-classification rule コマンドは分類ポリシーに AP 分類ルールを設定します。

undo apply ap-classification rule コマンドはデフォルトに戻します。

例

分類ポリシー**home** に AP classification rule 1 を設定します。不正な AP として AP classification rule 1 に一致する AP を指定します。重大度レベルを 80 に設定します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] apply ap-classification rule 1 rogue-ap severity-level 80

関連コマンド

ap-classification rule

2.1.7 apply classification policy

Syntax

apply classification policy *policy-name*

undo apply classification policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply classification policy コマンドは分類ポリシーを VSD（Virtual Security Domain）に適用します。

undo apply classification policy コマンドは VSD から分類ポリシーを削除します。

例

分類ポリシー**policy1** を VSD **home** に適用します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain home

[AP-wips-vsd-home] apply classification policy policy1

2.1.8 apply countermeasure policy

Syntax

apply countermeasure policy *policy-name*

undo apply countermeasure policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply countermeasure policy コマンドは対策ポリシーを VSD に適用します。

undo apply countermeasure policy コマンドは VSD から対策ポリシーを削除します。

例

対策ポリシー**policy2** を VSD **home** に適用します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain home

[AP-wips-vsd-home] apply countermeasure policy policy2

2.1.9 apply detect policy

Syntax

apply detect policy *policy-name*

undo apply detect policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply detect policy コマンドは攻撃検出ポリシーを VSD に適用します。

undo apply detect policy コマンドは VSD から攻撃検出ポリシーを削除します。

例

攻撃検出ポリシー**policy2** を VSD **home** に適用します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain home

[AP-wips-vsd-home] apply detect policy policy2

2.1.10 apply signature policy

Syntax

apply signature policy *policy-name*

undo apply signature policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply signature policy コマンドは署名ポリシーを VSD に適用します。

undo apply signature policy コマンドはデフォルトに戻します。

例

署名ポリシー**policy1** を VSD **home** に適用します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain home

[AP-wips-vsd-home] apply signature policy policy1

2.1.11 apply signature rule

Syntax

apply signature rule *rule-id*

undo apply signature rule *rule-id*

デフォルト

設定なし

View

Signature policy view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で署名を指定します。値の範囲は 1～65535 文字です。

説明

apply signature rule コマンドは署名ポリシーに署名を設定します。

undo apply signature rule コマンドはデフォルトに戻します。

例

signature 1 を署名ポリシー**office** に設定します。

<AP> system-view

[AP] wips

[AP-wips] signature policy office

[AP-wips-sig-office] apply signature rule 1

2.1.12 ap-rate-limit

Syntax

ap-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo ap-rate-limit

デフォルト

学習した AP エントリのための統計値収集間隔： 60 秒

遅延時間： 1200 秒

AP エントリしきい値： 64

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 学習した AP エントリのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS が AP エントリ攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold *threshold-value*: AP エントリ攻撃アラームを引き起こす AP エントリ数を指定します。*threshold-value* 引数の値の範囲は 1～4096 です。

説明

ap-rate-limit コマンドは AP エントリの学習を制限します。

undo ap-rate-limit コマンドはデフォルトに戻します。

例

AP エントリの学習を制限します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-rate-limit interval 60 quiet 1600 threshold 100

2.1.13 ap-spoofing

Syntax

ap-spoofing [**quiet** *quiet-value*]

undo ap-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP スプーフィング攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こしません。

説明

ap-spoofing コマンドは AP スプーフィング攻撃を有効にします。

undo ap-spoofing コマンドは AP スプーフィング攻撃を無効にします。

例

AP スプーフィング検出を有効にし、遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-spoofing quiet 360

2.1.14 ap-timer

Syntax

ap-timer [**inactive** *inactive-value* **aging** *aging-value*]

undo ap-timer

デフォルト

非アクティブ時間： 300 秒

エージングタイマ： 600 秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

inactive *inactive-value*: 非アクティブ時間を指定します。*inactive-value* 引数の値の範囲は 60～1200 秒です。指定された非アクティブ時間内に AP がフレームを送受信しない場合、WIPS は AP を非アクティブ状態に設定します。

aging *aging-value*: エージングタイマを指定します。値の範囲は 120～86400 秒です。指定されたエージングタイマ内に AP がフレームを送受信しない場合、WIPS はエントリを削除します。エージングタイマは非アクティブ時間より大きくなければなりません。

説明

ap-timer コマンドは AP エントリタイマを設定します。

undo ap-timer コマンドはデフォルトに戻します。

例

非アクティブ時間を 120 秒、エージングタイマを 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-timer inactive 120 aging 360

2.1.15 association-table-overflow

Syntax

association-table-overflow [**quiet** *quiet-value*]

undo association-table-overflow

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がアソシエーション/再アソシエーション DoS 攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にアソシエーション/再アソシエーション DoS 攻撃を検出してもアラームを引き起こしません。

説明

association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を設定します。

undo association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を無効にします。

例

アソシエーション/再アソシエーション DoS 攻撃検出を有効にし、遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] association-table-overflow quiet 100

2.1.16 authentication

Syntax

authentication { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }

undo authentication

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

equal: 指定された認証モードと等しい認証モードを整合します。

include: 指定された認証モードを含む認証モードを整合します。

802.1x: 802.1X 認証モードを指定します。

none: 認証モードは指定されません。

other: 802.1X と PSK 以外の認証モードを指定します。

psk: PSK 認証モードを指定します。

説明

authentication コマンドは AP の認証モードを整合するために AP 分類ルールを設定します。

undo authentication コマンドはデフォルトに戻します。

例

PSK 認証モードを使用する AP を整合するために AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] authentication equal psk

2.1.17 block mac-address

Syntax

block mac-address *mac-address*

undo block mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

all: すべての MAC アドレスを指定します。

説明

block mac-address コマンドはスタティック禁止装置リストに AP もしくはクライアントの MAC アドレスを追加します。

undo block mac-address コマンドはスタティック禁止装置リストから 1 つもしくはすべての MAC アドレスを削除します。

例

スタティック禁止装置リストに MAC アドレス **78AC-C0AF-944F** を追加します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] block mac-address 78AC-C0AF-944F

2.1.18 classification policy

Syntax

classification policy *policy-name*

undo classification policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

classification policy コマンドは分類ポリシーを作成し、その view に移行します。

undo classification policy コマンドは分類ポリシーを削除します。

例

分類ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home]

2.1.19 client-association fast-learn enable

Syntax

client-association fast-learn enable

undo client-association fast-learn enable

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

説明

client-online コマンドはクライアントアソシエーションエントリの高速学習を有効します。

クライアントアソシエーションエントリは、クライアントが AP にアソシエートした後に AC に保存されるエントリです。

このコマンドが設定されていない場合、センサがクライアントアソシエーションエントリを学習できるのは、クライアントが AP に正常にアソシエートされた後だけです。このコマンドが設定されると、センサはアソシエーションプロセス中にクライアントアソシエーションエントリを学習できます。

センサがアソシエーションプロセス中にクライアントアソシエーションエントリを学習した場合、センサは AP とクライアント間のアソシエーション要求または応答を検出するたびにエントリを更新します。

このコマンドにより、アソシエーションの効率は向上しますが、アソシエーションの精度は低下します。ベストプラクティスとして、ネットワークで高速な攻撃の検出と対策が必要な場合にのみ、このコマンドを設定します。

例

クライアントアソシエーションエントリの高速学習を有効にします。

<AP> system-view

[AP] wips

[AP-wips] detect policy

2.1.20 client-online

Syntax

client-online *value1* [**to** *value2*]

undo client-online

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 **to** *value2*: AP に紐付けられたクライアント数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～128 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

client-online コマンドは AP に紐付いたクライアント数を整合するために AP 分類ルールを設定します。

undo client-online コマンドはデフォルトに戻します。

例

20～40 のクライアントに紐付いた AP を整合するために、AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] client-online 20 to 40

2.1.21 client-rate-limit

Syntax

client-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo client-rate-limit

デフォルト

学習したクライアントエントリのための統計値収集間隔： 60 秒

遅延時間： 1200 秒

クライアントエントリしきい値： 512

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 学習したクライアントエントリのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS がクライアントエントリ攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内にクライアントエントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold *threshold-value*: クライアントエントリ攻撃アラームを引き起こすクライアントエントリ数を指定します。*threshold-value* 引数の値の範囲は 1～4096 です。

説明

client-rate-limit コマンドはクライアントエントリの学習を制限します。

undo client-rate-limit コマンドはデフォルトに戻します。

例

クライアントエントリの学習を制限します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] client-rate-limit interval 80 quiet 1600 threshold 100

2.1.22 client-spoofing

Syntax

client-spoofing [**quiet** *quiet-value*]

undo client-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がクライアントスプーフィング攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にクライアントスプーフィング攻撃を検出してもアラームを引き起こしません。

説明

client-spoofing コマンドはクライアントスプーフィング攻撃検出を有効にします。

undo client-spoofing コマンドはクライアントスプーフィング攻撃検出を無効にします。

例

クライアントスプーフィング攻撃検出を有効にし、遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] client-spoofing quiet 360

2.1.23 client-timer

Syntax

client-timer inactive *inactive-value* **aging** *aging-value*

undo client-timer

デフォルト

非アクティブ時間： 300 秒

エージングタイマ： 600 秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

inactive *inactive-value*: 非アクティブ時間を指定します。*inactive-value* 引数の値の範囲は 60～1200 秒です。指定された非アクティブ時間内にクライアントがフレームを送受信しない場合、WIPS はクライアントを非アクティブ状態に設定します。

aging *aging-value*: エージングタイマを指定します。値の範囲は 120～86400 秒です。指定されたエージングタイマ内にクライアントがフレームを送受信しない場合、WIPS はエントリを削除します。エージングタイマは非アクティブ時間より大きくなければなりません。

説明

client-timer コマンドはクライアントエントリタイマを設定します。

undo client-timer コマンドはデフォルトに戻します。

例

非アクティブ時間を 120 秒、エージングタイマを 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] client-timer inactive 120 aging 360

2.1.24 countermeasure adhoc

Syntax

countermeasure adhoc

undo countermeasure adhoc

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure adhoc コマンドはアドホックデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure adhoc コマンドはデフォルトに戻します。

例

アドホックデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure adhoc

2.1.25 countermeasure attack all

Syntax

countermeasure attack all

undo countermeasure attack all

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack all コマンドはすべての攻撃者に対策を講じるために WIPS を有効にします。

undo countermeasure attack all コマンドはデフォルトに戻します。

例

すべての攻撃者に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack all

2.1.26 countermeasure attack deauth-broadcast

Syntax

countermeasure attack deauth-broadcast

undo countermeasure attack deauth-broadcast

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure deauth-broadcast コマンドはブロードキャスト認証解除攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure deauth-broadcast コマンドはデフォルトに戻します。

例

ブロードキャスト認証解除攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack deauth-broadcast

2.1.27 countermeasure attack disassoc-broadcast

Syntax

countermeasure attack disassoc-broadcast

undo countermeasure attack disassoc-broadcast

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack disassoc-broadcast コマンドはブロードキャストディスアソシエーション攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack disassoc-broadcast コマンドはデフォルトに戻します。

例

ブロードキャストディスアソシエーション攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack disassoc-broadcast

2.1.28 countermeasure attack honeypot-ap

Syntax

countermeasure attack honeypot-ap

undo countermeasure attack honeypot-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack honeypot-ap コマンドはハニーポット AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack honeypot-ap コマンドはデフォルトに戻します。

例

ハニーポット AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack honeypot-ap

2.1.29 countermeasure attack hotspot-attack

Syntax

countermeasure attack hotspot-attack

undo countermeasure attack hotspot-attack

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack hotspot-attack コマンドはホットスポット攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack hotspot-attack コマンドはデフォルトに戻します。

例

ホットスポット攻撃を開始するデバイスに対策を講じるためにWIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack hotspot-attack

2.1.30 countermeasure attack ht-40-mhz-intolerance

Syntax

countermeasure attack ht-40-mhz-intolerance

undo countermeasure attack ht-40-mhz-intolerance

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack ht-40-mhz-intolerance コマンドは 40MHz 帯域幅モードが無効のデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack ht-40-mhz-intolerance コマンドはデフォルトに戻します。

例

40MHz 帯域幅モードが無効のデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack ht-40-mhz-intolerance

2.1.31 countermeasure attack malformed-packet

Syntax

countermeasure attack malformed-packet

undo countermeasure attack malformed-packet

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack malformed-packet コマンドは不正な形式のパケットを送信するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack malformed-packet コマンドはデフォルトに戻します。

例

不正な形式のパケットを送信するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack malformed-packet

2.1.32 countermeasure attack man-in-the-middle

Syntax

countermeasure attack man-in-the-middle

undo countermeasure attack man-in-the-middle

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack man-in-the-middle コマンドは MITM 攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack man-in-the-middle コマンドはデフォルトに戻します。

例

MITM 攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack man-in-the-middle

2.1.33 countermeasure attack omerta

Syntax

countermeasure attack omerta

undo countermeasure attack omerta

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack omerta コマンドは Omerta 攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack omerta コマンドはデフォルトに戻します。

例

Omerta 攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack omerta

2.1.34 countermeasure attack power-save

Syntax

countermeasure attack power-save

undo countermeasure attack power-save

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack power-save コマンドは節電攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack power-save コマンドはデフォルトに戻します。

例

節電攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack power-save

2.1.35 countermeasure attack soft-ap

Syntax

countermeasure attack soft-ap

undo countermeasure attack soft-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack soft-ap コマンドはソフト AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack soft-ap コマンドはデフォルトに戻します。

例

ソフト AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack soft-ap

2.1.36 countermeasure attack unencrypted-trust-client

Syntax

countermeasure attack unencrypted-trust-client

undo countermeasure attack unencrypted-trust-client

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack unencrypted-trust-client コマンドは暗号化されていない許可されたクライアントに対策を講じるために WIPS を有効にします。

undo countermeasure attack unencrypted-trust-client コマンドはデフォルトに戻します。

例

暗号化されていない許可されたクライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack unencrypted-trust-client

2.1.37 countermeasure attack weak-iv

Syntax

countermeasure attack weak-iv

undo countermeasure attack weak-iv

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack weak-iv コマンドは Weak IV を使用するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack weak-iv コマンドはデフォルトに戻します。

例

Weak IV を使用するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack weak-iv

2.1.38 countermeasure attack windows-bridge

Syntax

countermeasure attack windows-bridge

undo countermeasure attack windows-bridge

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack windows-bridge コマンドは Windows ブリッジ攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack windows-bridge コマンドはデフォルトに戻します。

例

Windows ブリッジ攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack windows-bridge

2.1.39 countermeasure enhance

Syntax

countermeasure enhance

undo countermeasure enhance

デフォルト

エンハンスされた対策モードは、無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

エンハンスされた対策モードを有効にするには、**countermeasure enhance** します。

undo countermeasure enhance を使用してデフォルトに戻します。

このコマンドを設定して、デュアルバンド クライアントが不正 AP 上の同じ SSID を共有する 2 つの無線間でローミングできないようにします。

例

エンハンスされた対策モードを有効にします。

```
<AP> system-view
[AP] wips
[AP-wips] countermeasure policy home
[AP-wips-cms-home] countermeasure enhance
```

2.1.40 countermeasure external-ap

Syntax

countermeasure external-ap

undo countermeasure external-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure external-ap コマンドは外部の AP に対策を講じるために WIPS を有効にします。

undo countermeasure external-ap コマンドはデフォルトに戻します。

例

#外部の AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure external-ap

2.1.41 countermeasure mac-address

Syntax

countermeasure mac-address *mac-address*

undo countermeasure mac-address { *mac-address* | **all** }

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

all: すべての AP とクライアントを指定します。

説明

countermeasure mac-address コマンドは指定された MAC アドレスを持つ装置に対策を講じるために WIPS を有効にします。

undo countermeasure mac-address コマンドは設定を削除します。

countermeasure mac-address コマンドを複数回設定することで、複数の装置に対策を講じるように WIPS を有効化できます。

例

MAC アドレス **2a11-1fa1-141f** を持つ装置に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure mac-address 2a11-1fa1-141f

2.1.42 countermeasure misassociation-client

Syntax

countermeasure misassociation-client

undo countermeasure misassociation-client

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure misassociation-client コマンドは間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

undo countermeasure misassociation-client コマンドはデフォルトに戻します。

例

間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure misassociation-client

2.1.43 countermeasure misconfigured-ap

Syntax

countermeasure misconfigured-ap

undo countermeasure misconfigured-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure misconfigured-ap コマンドは間違って設定された AP に対策を講じるために WIPS を有効にします。

undo countermeasure misconfigured-ap コマンドはデフォルトに戻します。

例

間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure misconfigured-ap

2.1.44 countermeasure packet-sending-interval

Syntax

countermeasure packet-sending-interval *interval*

undo countermeasure packet-sending-interval

デフォルト

30 ミリ秒

View

Countermeasure policy view

定義済みユーザロール

network-admin

パラメータ

interval: センサが対策パケットを送信する間隔を指定します。値の範囲は 1~100 ミリ秒です。

説明

countermeasure policy コマンドは、センサが対策パケットを送信する間隔を指定します。

undo countermeasure policy コマンドは、対策ポリシーを削除します。

チャネル内に不正デバイスが検出された場合に、センサがチャネル内で対策パケットを送信できるようにするには、このコマンドを設定します。センサはスキャン期間内にのみチャネル内で対策パケットを送信し、センサが対策パケットを送信する間隔を指定できます。チャネルスキャンの詳細については、コマンドマニュアルのセクション 8 の *Radio リソース管理 "Radio リソース管理"* を参照してください。

例

10 ミリ秒ごとに対策パケットを送信するようにセンサを設定します。

<AP> system-view

[AP] wips

[AP] countermeasure policy home

[AP-wips-cms-home] countermeasure packet-sending-interval 10

2.1.45 countermeasure policy

Syntax

countermeasure policy *policy-name*

undo countermeasure policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 対策ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

countermeasure policy コマンドは対策ポリシーを作成し、その view に移行します。

undo countermeasure policy コマンドは対策ポリシーを削除します。

例

対策ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home]

2.1.46 countermeasure potential-authorized-ap

Syntax

countermeasure potential-authorized-ap

undo countermeasure potential-authorized-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-authorized-ap コマンドは潜在的に認可された AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-authorized-ap コマンドはデフォルトに戻します。

例

潜在的に認可された AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure potential-authorized-ap

2.1.47 countermeasure potential-external-ap

Syntax

countermeasure potential-external-ap

undo countermeasure potential-external-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-external-ap コマンドは潜在的外部 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-external-ap コマンドはデフォルトに戻します。

例

対策ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure potential-external-ap

2.1.48 countermeasure potential-rogue-ap

Syntax

countermeasure potential-rogue-ap

undo countermeasure potential-rogue-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-rogue-ap コマンドは潜在的な不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-rogue-ap コマンドはデフォルトに戻します。

例

潜在的な不正 AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure potential-rogue-ap

2.1.49 countermeasure rogue-ap

Syntax

countermeasure rogue-ap

undo countermeasure rogue-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure rogue-ap コマンドは不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure rogue-ap コマンドはデフォルトに戻します。

例

不正な AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure rogue-ap

2.1.50 countermeasure unauthorized-client

Syntax

countermeasure unauthorized-client

undo countermeasure unauthorized-client

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure unauthorized-client コマンドは未許可クライアントに対策を講じるために WIPS を有効にします。

undo countermeasure unauthorized-client コマンドはデフォルトに戻します。

例

未許可クライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure unauthorized-client

2.1.51 countermeasure uncategorized-ap

Syntax

countermeasure uncategorized-ap

undo countermeasure uncategorized-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure uncategorized-ap コマンドは未分類の AP に対策を講じるために WIPS を有効にします。

undo countermeasure uncategorized-ap コマンドはデフォルトに戻します。

例

未分類の AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure uncategorized-ap

2.1.52 countermeasure uncategorized-client

Syntax

countermeasure uncategorized-client

undo countermeasure uncategorized-client

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure uncategorized-client コマンドは未分類のクライアントに対策を講じるために WIPS を有効にします。

undo countermeasure uncategorized-client コマンドはデフォルトに戻します。

例

未分類のクライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure uncategorized-client

2.1.53 deauthentication-broadcast

Syntax

deauthentication-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo deauthentication-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証取り消し攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。WIPS は遅延時間内にブロードキャスト認証取り消し攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証取り消し攻撃アラームを引き起こすブロードキャスト認証取り消しの数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

deauthentication-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を設定します。

undo deauthentication-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を無効にします。

例

ブロードキャスト認証取り消し攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] deauthentication-broadcast interval 100 threshold 100 quiet 360

2.1.54 deauth-spoofing

Syntax

deauth-spoofing [**quiet** *quiet*]

undo deauth-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet*: スプーフィング認証解除フレームで WIPS がアラームをトリガーした後の待機時間を指定します。*quiet-value* 引数の値の範囲は 5~604800 秒で、デフォルトの待機時間は 600 秒です。WIPS は、待機時間内にスプーフィング認証解除フレームを検出してもアラームをトリガーしません。

説明

deauth-spoofing コマンドはスプーフィング認証解除フレーム検出を設定します。

undo deauth-spoofing コマンドはスプーフィング認証解除フレーム検出を無効にします。

例

スプーフィング認証解除フレーム検出を有効にし、クワイエットタイムを 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] deauth-spoofing quiet 100

2.1.55 detect dissociate-client enable

Syntax

detect dissociate-client enable

undo detect dissociate-client enable

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

説明

detect policy コマンドは WIPS が関連付けられていないクライアントを検出できるようにします。

undo detect policy コマンドは WIPS が関連付けられていないクライアントを検出できないようにします。

例

関連付けられていないクライアントを検出するために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] detect dissociate-client enable

2.1.56 detect policy

Syntax

detect policy *policy-name*

undo detect policy *policy-name*

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

policy-name: 攻撃検出ポリシー名を指定します。大文字と小文字を区別します。設定範囲は 1～63 文字です。

説明

detect policy コマンドは攻撃検出ポリシーを作成し、その view に移行します。

undo detect policy コマンドは攻撃検出ポリシーを削除します。

例

攻撃検出ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home]

2.1.57 detect signature

Syntax

detect signature [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo detect

デフォルト

有効

View

Signature policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 署名に一致するパケットのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が user-defined 攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内に user-defined 攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: user-defined 攻撃アラームを引き起こす、署名に一致したパケット数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

detect signature コマンドは署名に基づく user-define 攻撃検出を有効にします。

undo detect signature コマンドは署名に基づく user-define 攻撃検出を無効にします。

例

署名に基づく user-define 攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、60、100、360 に設定します。

<AP> system-view

[AP] wips

[AP-wips] signature policy home

[AP-wips-sig-home] detect signature interval 60 threshold 100 quiet 360

2.1.58 disassociation-broadcast

Syntax

disassociation-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo disassociation-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証取り消し攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内にブロードキャスト認証取り消し攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証取り消し攻撃アラームを引き起こす、ブロードキャスト認証取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

disassociation-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を有効にします。

undo disassociation-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を無効にします。

例

ブロードキャスト認証取り消し攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] disassociation-broadcast interval 100 threshold 100 quiet 360

2.1.59 discovered-ap

Syntax

discovered-ap *value1* [**to** *value2*]

undo discovered-ap

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 **to** *value2*: AP を検出するセンサの数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 1～128 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

discovered-ap コマンドは AP を検出するセンサの数を整合するために AP 分類ルールを設定します。

undo discovered-ap コマンドはデフォルトに戻します。

例

10～128 のセンサに検出された AP を整合するために、AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] discovered-ap 10 to 128

2.1.60 display wips sensor

Syntax

display wips sensor

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wips sensor コマンドはすべてのセンサに関する情報を表示します。

例

すべてのセンサに関する情報を表示します。

<AP> display wips sensor

```
Total number of sensors: 1
Sensor ID    Sensor name             VSD name            Radio ID   Status
3            fatap                   aaa                 1          Active
```

表 2-1 コマンド出力

フィールド	説明
VSD name	APが属するVSDの名前
Radio ID	WIPSで有効化された無線の名前
Status	センサの状態 ● **Active**－センサはWIPSで有効にされます。 ● **Inactive**－センサはWIPSで有効にされません。

2.1.61 display wips statistics

Syntax

display wips statistics [**receive** | **virtual-security-domain** *vsd-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

receive: すべての VSD のセンサから AC が受信する攻撃検出統計値情報を表示します。

virtual-security-domain *vsd-name*: 指定された VSD のセンサから AC が受信する攻撃検出統計値情報を表示します。

説明

display wips statistics コマンドはセンサから収集した攻撃検出情報を表示します。

例

すべての VSD のセンサから収集した攻撃検出統計値情報を表示します。

<AP> display wips statistics receive

```
Information from sensor 1
 Information about attack statistics:
   Detected association-request flood messages: 0
   Detected authentication flood messages: 0
   Detected beacon flood messages: 0
   Detected block-ack flood messages: 0
   Detected cts flood messages: 0
   Detected deauthentication flood messages: 0
   Detected disassociation flood messages: 0
   Detected eapol-start flood messages: 0
   Detected null-data flood messages: 0
   Detected probe-request flood messages: 0
   Detected reassociation-request flood messages: 0
   Detected rts flood messages: 0
   Detected eapol-logoff flood messages: 0
   Detected eap-failure flood messages: 0
   Detected eap-success flood messages: 0
   Detected duplicated-ie messages: 0
   Detected fata-jack messages: 0
```

```
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected signature rule messages: 0
Detected 40MHZ messages: 0
Detected power save messages: 0
Detected omerta messages: 0
Detected windows bridge messages: 0
Detected soft AP messages: 0
Detected broadcast disassociation messages: 0
Detected broadcast deauthentication messages: 0
Detected AP impersonate messages: 0
Detected illegal channel 9 messages: 1
```

表 2-2 コマンド出力

フィールド	説明
Information from sensor n	センサ**n** から収集した情報。**n** はセンサのIDをあらわします。
Detected association-request flood messages	紐付け要求フラッドアタック攻撃に対して検出したメッセージの数。
Detected authentication flood messages	認証要求フラッド攻撃に対して検出したメッセージの数。
Detected beacon flood messages	ビーコンフラッド攻撃に対して検出したメッセージの数。

フィールド	説明
Detected block-ack flood messages	ブロックアクトフラッド攻撃に対して検出したメッセージの数。
Detected cts flood messages	CTSフラッド攻撃に対して検出したメッセージの数。
Detected deauthentication flood messages	認証取り消しフラッド攻撃に対して検出したメッセージの数。
Detected disassociation flood messages	紐付け取り消しフラッド攻撃に対して検出したメッセージの数。
Detected eapol-start flood messages	EAPOLスタートフラッド攻撃に対して検出したメッセージの数。
Detected null-data flood messages	ヌルデータフラッド攻撃に対して検出したメッセージの数。
Detected probe-request flood messages	プローブ要求フラッド攻撃に対して検出したメッセージの数。
Detected reassociation-request flood messages	再紐付け要求フラッド攻撃に対して検出したメッセージの数。
Detected rts flood messages	RTSフラッド攻撃に対して検出したメッセージの数。
Detected eapol-logoff flood messages	EAPOLログオフフラッド攻撃に対して検出したメッセージの数。
Detected eap-failure flood messages	EAPOL失敗フラッド攻撃に対して検出したメッセージの数。
Detected eap-success flood messages	EAPOL成功フラッド攻撃に対して検出したメッセージの数。
Detected duplicated-ie messages	複製されたIEをもつ異常パケットに対して検出したメッセージの数。
Detected fata-jack messages	FATAジャック異常パケットに対して検出したメッセージの数。
Detected illegal-ibss-ess messages	異常なIBSSとESS設定をもつ異常パケットに対して検出したメッセージの数。
Detected invalid-address-combination messages	無効な送信元アドレスをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-assoc-req messages	異常な紐付け要求に対して検出したメッセージの数。
Detected invalid-auth messages	異常な認証要求に対して検出したメッセージの数。
Detected invalid-deauth-code messages	無効な認証取り消しコードをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-disassoc-code messages	無効な紐付け取り消しコードをもつ異常パケットに対して検出したメッセージの数。

フィールド	説明
Detected invalid-ht-ie messages	異常なHT IEをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-ie-length messages	無効なIE長をもつ異常パケットに対して検出したメッセージの数。
Detected invalid-pkt-length messages	無効なパケット長をもつ異常パケットに対して検出したメッセージの数。
Detected large-duration messages	オーバーサイズの期間をもつ異常パケットに対して検出したメッセージの数。
Detected null-probe-resp messages	異常なプローブ要求フレームに対して検出したメッセージの数。
Detected overflow-eapol-key messages	オーバーサイズのEAPOL鍵をもつ異常パケットに対して検出したメッセージの数。
Detected overflow-ssid messages	オーバーサイズなSSIDをもつ異常パケットに対して検出したメッセージの数。
Detected redundant-ie messages	冗長なIEをもつ異常パケットに対して検出したメッセージの数。
Detected AP spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs AP)
Detected AP spoof client messages	クライアントスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs client)
Detected AP spoof ad-hoc messages	アドホックスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs Ad hoc)
Detected ad-hoc spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(Ad hoc spoofs AP)
Detected client spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(client spoofs AP)
Detected weak IV messages	ウィークIVに対して検出したメッセージの数。
Detected excess AP messages	APエントリ攻撃に対して検出したメッセージの数。
Detected excess client messages	クライアントエントリ攻撃に対して検出したメッセージの数。
Detected 40MHZ messages	40Hz帯モードで無効化されるクライアントに対して検出したメッセージの数。
Detected power save messages	電力節約攻撃に対して検出したメッセージの数。
Detected omerta messages	Omerta攻撃に対して検出したメッセージの数。
Detected windows bridge messages	Windowsブリッジに対して検出したメッセージの数。
Detected soft AP messages	ソフトAPに対して検出したメッセージの数。

フィールド	説明
Detected broadcast disassociation messages	ブロードキャスト紐付け取り消し攻撃に対して検出したメッセージの数。
Detected broadcast deauthentication messages	ブロードキャスト認証取り消し攻撃に対して検出したメッセージの数。
Detected AP impersonate messages	APなりすまし攻撃に対して検出したメッセージの数。
Detected illegal channel n messages:	禁止されたチャネルに対して検出したメッセージの数。*n*はチャネル番号を示します。

関連コマンド

reset wips statistics

2.1.62 display wips virtual-security-domain countermeasure record

Syntax

display wips virtual-security-domain *vsd-name* **countermeasure record**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

display wips virtual-security-domain countermeasure record コマンドは不正なデバイスに対して WIPS が実行した対策に関する情報が表示されます。

例

WIPS が VSD **office** の不正デバイスに対して行った対策に関する情報を表示します。

<AP> display wips virtual-security-domain office countermeasure record

Total 3 times countermeasure, current 3 countermeasure record in virtual-security-domain office

Reason: Att - attack; Ass - associated; Black - blacklist;

Class - classification; Manu - manual;

MAC address	Type	Reason	Countermeasure AP	Radio ID	Time
1000-0000-00e3	AP	Manu	fatap	1	2020-05-03/09:32:01
1000-0000-00e4	AP	Manu	fatap	1	2020-05-03/09:32:11
2000-0000-f282	Client	Black	fatap	1	2020-05-03/09:31:56

表 2-3 コマンド出力

フィールド	説明
Total *number* times countermeasure, current *number* countermeasure record in virtual-security-domain *name*	成功した対策の数です。このフィールドには、最大1024件の対策レコードを表示できます。
MAC Address	WIPSが対策を講じた無線装置のMACアドレスです。
Type	ワイヤレス装置のタイプ:APまたはクライアントです。
Reason	WIPSがワイヤレス装置対策を行う理由: • **Att**－WIPSは装置が攻撃者であるために対策を講じています。 • **Class** — WIPSは装置に対して装置型をベースにした対抗策をとっています。 • **Manu** — WIPSは装置アドレスに基づいてMACへの対抗策をとります。
Countermeasure AP	無線装置対策センサの名称です。
Radio ID	無線装置対策を行うセンサの無線IDです。
Time	無線装置対策をセンサに通知する時間です。

関連コマンド

reset wips virtual-security-domain countermeasure record

2.1.63 display wips virtual-security-domain device

Syntax

display wips virtual-security-domain *vsd-name* **device** [**ap** [**ad-hoc | authorized | external | mesh | misconfigured | potential-authorized | potential-external | potential-rogue | rogue | uncategorized**] **| client** [[**dissociative-client**] **|** [**authorized | misassociation | unauthorized | uncategorized**]] **| mac-address** *mac-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 無線装置の情報を表示します。

ap: AP の情報を表示します。

ad-hoc: アドホックモードで動作する AP に関する情報を表示します。

authorized: 許可 AP に関する情報を表示します。

external: 外部 AP に関する情報を表示します。

mesh: MP に関する情報を表示します。

misconfigured: 間違って設定された AP に関する情報を表示します。

potential-authorized: 潜在的に許可された AP に関する情報を表示します。

potential-rogue: 潜在的な不正 AP に関する情報を表示します。

potential-external: 潜在的外部 AP に関する情報を表示します。

rogue: 不正な AP に関する情報を表示します。

uncategorized: 分類されていない AP に関する情報を表示します。

client: クライアント情報を表示します。

dissociative-client: 紐付けられていないクライアント情報を表示します。

authorized: 許可クライアントに関する情報を表示します。

misassociation: 間違って紐付けられたクライアントに関する情報を表示します。

unauthorized: 未許可クライアントに関する情報を表示します。

uncategorized: 分類されていないクライアントに関する情報を表示します。

mac-address *mac-address*: 特定の無線装置に関する情報を表示します。*mac-address* 引数は無線装置の MAC アドレスを表し、H-H-H 形式です。

verbose: 詳細な装置情報を表示します。

説明

display wips virtual-security-domain device コマンドは VSD で検出された無線装置に関する情報を表示します。

例

VSD **office** で検出された無線装置に関する情報を表示します。

<AP> display wips virtual-security-domain office device

```
Total 3 detected devices in virtual-security-domain office

Class: Auth - authorization; Ext - external; Mis - mistake;
      Unauth - unauthorized; Uncate - uncategorized;
      (A) - associate; (C) - config; (P) - potential;
      Ad-hoc; Mesh

MAC address    Type   Class    Duration    Sensors Channel Status
1000-0000-0000 AP     Ext(P)   00h 10m 46s 1       11      Active
1000-0000-0001 AP     Ext(P)   00h 10m 46s 1       6       Active
1000-0000-0002 AP     Ext(P)   00h 10m 46s 1       1       Active
```

表 2-4 コマンド出力

フィールド	説明
Type	無線装置タイプ： AP、Client、またはMesh
Class	無線装置のカテゴリ
Duration	無線装置が現在の状態に移行してからの期間
Sensors	無線装置を検出したセンサの数
Channel	直近で無線装置が検出されたチャネル
Status	APもしくはクライアントの状態 ● **Active**－APもしくはクライアントはアクティブです。 ● **Inactive**－APもしくはクライアントは非アクティブです。

VSD **a** で検出された無線装置に関する詳細な情報を表示します。

<AP> display wips virtual-security-domain a device verbose

```
Total 2 detected devices in virtual-security-domain a
```

```
 AP: 1000-0000-0000
   Mesh Neighbor: None
   Classification: Mis(C)
   Severity level: 0
   Classify way: Auto
   Status: Active
   Status duration: 00h 27m 57s
   Vendor: Not found
   SSID: service
   Radio type: 802.11g
   Countermeasuring: No
   Security: None
   Encryption method: None
   Authentication method: None
   Broadcast SSID: Yes
   QoS supported: No
   Ad-hoc: No
   Beacon interval: 100 TU
   Up duration: 00h 27m 57s
Channel band-width supported: 20MHZ
   Hotspot AP: No
   Soft AP: No
   Honeypot AP: No
   Total number of reported sensors: 1
     Sensor 1:
       Sensor ID: 1
       Sensor name: fatap
       Radio ID: 1
       RSSI: 15
       Channel: 64
       First reported time: 2014-06-03/09:05:51
       Last reported time: 2014-06-03/09:05:51
   Total number of associated clients: 1
     01: 2000-0000-0000
Client: 2000-0000-0000
  Last reported associated AP: 1000-0000-0000
  Classification: Uncate
  Severity level: 0
  Classify way: Auto
  Dissociative status: No
  Status: Active
  Status duration: 00h 00m 02s
```

```
Vendor: Not found
Radio type: 802.11a
40MHz intolerance: No
Countermeasuring: No
Man in the middle: No
Total number of reported sensors: 1
   Sensor 1:
     Sensor ID: 1
     Sensor name: fatap
     Radio ID: 1
     RSSI: 50
     Channel: 64
     First reported time: 2014-06-03/14:52:56
     Last reported time: 2014-06-03/14:52:56
     Reported associated AP: 1000-0000-0000
```

表 2-5 コマンド出力

フィールド	説明
AP	APのMACアドレス
Mesh Neighbor	メッシュAPのネイバのMACアドレス
Client	クライアントのMACアドレス
Last reported associated AP	クライアントが直近で報告した、紐付けられたAPのMACアドレス

フィールド	説明

Classification	APもしくはクライアントのカテゴリ
	• APカテゴリオプション
	  • ad_hoc
	  • authorized
	  • rogue
	  • misconfigured
	  • external
	  • potential-authorized
	  • potential-rogue
	  • potential-external
	  • uncategorized
	• クライアントカテゴリオプション
	  • authorized
	  • unauthorized
	  • misassociated
	  • uncategorized

Severity level	装置の重大度レベル
Classify way	APもしくはクライアント分類方法 • **Manual**－手動分類 • **Invalid OUI**－無効なOUIリストに追加 • **Block List**－禁止装置リストに追加 • **Trust List**－許可装置リストに追加 • **User Define**－ユーザが定義した分類 • **Auto**－自動分類
Dissociative status	クライアントが紐付けられたものではないかどうかをあらわします。
Status	APもしくはクライアントの状態 • **Active**－APもしくはクライアントはアクティブです。 • **Inactive**－APもしくはクライアントは非アクティブです。
Status duration	無線装置が現在の状態に移行してからの期間
Vendor	装置のOUI。装置のOUIが、インポートされたOUIと一致する場合、このフィールドは装置のOUIを表示します。装置にOUIが設定されていない場合、あるいは装置のOUIが、インポートされたいずれのOUIとも一致しない場合、このフィールドは**Not found**を表示します。

フィールド	説明
SSID	APに提供された無線装置のSSID
Radio Type	無線装置の無線モード
40MHz intolerance	クライアントが40MHz帯をサポートするかどうかをあらわします。
Countermeasuring	WIPSが無線装置に対策を講じるかをあらわします。 ● No ● Yes
Man in the middle	MITM攻撃を検出するかどうかをあらわします。
Security	セキュリティ方式。 ● None ● WEP ● WPA ● WPA2
Encryption method	データ暗号方式。 ● TKIP ● CCMP ● WEP ● None
Authentication method	認証方式。 ● None ● PSK ● 802.1X ● Others－PSK認証と802.1X認証以外の認証方式
Broadcast SSID	APがSSIDをブロードキャストするかどうかをあらわします。APがSSIDをブロードキャストしない場合、このフィールドは何も表示しません。
QoS supported	無線装置がQoSをサポートするかどうかをあらわします。
Ad-hoc	無線装置がアドホックモードかどうかをあらわします。
Beacon interval	TUにおけるビーコン間隔です。1つのTUは1024マイクロ秒に等しいです。
Channel band-width supported	サポートされたチャネル帯域幅モード ● 20/40/80MHZ ● 20/40MHz ● 20MHz

フィールド	説明
Hotspot AP	APがホットスポット攻撃APであるかどうかをあらわします。
Soft AP	APがソフトAPであるかどうかをあらわします。
Honeypot AP	APがハニーポットAPであるかどうかをあらわします。
Sensor n	無線装置を検出したセンサです。n はシステムに割り当てられたIDをあらわします。
Channel	センサが直近で無線装置を検出したチャネルです。
First reported time	センサが最初に無線装置を検出した時間です。
Last reported time	センサが直近で無線装置を検出した時間です。
n: H-H-H	APに紐付けられたMACアドレスです。n はシステムに割り当てられたIDをあらわします。
Reported associated AP	センサが報告した、紐付けられたAPのMACアドレスです。

関連コマンド

reset wips virtual-security-domain device

2.1.64 embedded-oui-classify enable

Syntax

embedded-oui-classify enable

デフォルト

設定なし

View

Device category view

定義済みユーザロール

network-admin

説明

flood association-request コマンドは WIPS OUI ライブラリの内蔵 OUI に基づいてデバイスを分類します。

例

装置分類ポリシー**home** の WIPS OUI ライブラリの組み込み OUI に基づく装置分類を有効にします。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] embedded-oui-classify enable

関連コマンド

reset wips embedded-oui

2.1.65 export oui

Syntax

export oui *file-name*

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: 設定ファイルを名前で指定します。大文字と小文字は区別されず、1~255 文字の文字列で指定します。バックスラッシュ(¥)、スラッシュ(/)、コロン (:) 、アスタリスク(*)、疑問符 (?)、引用符(")、左山括弧 (<) 、右山括弧(>) 、縦棒(|)は使用できません。

説明

export oui コマンドは OUI ライブラリ内のすべての OUI を OUI 設定ファイルにエクスポートします。

このコマンドは、埋め込み OUI とインポートされた OUI を含むすべての OUI をエクスポートします。

OUI は次の形式でエクスポートされます。

```
000FE2 (base 16) New H3C Technologies Co., Ltd..
```

例

OUI ライブラリ内のすべての OUI を構成ファイル **OUIInfo** にエクスポートします。

<AP> system-view

[AP] wips

[AP-wips] export oui OUIInfo

関連コマンド

- i**mport oui**
- **reset wips embedded-oui**

2.1.66 flood association-request

Syntax

flood association-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood association-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 紐付け要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が紐付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に紐付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 紐付け要求フラッド攻撃アラームを引き起こす紐付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood association-request コマンドは紐付け要求フラッド攻撃検出を設定します。

undo flood association-request コマンドはデフォルトに戻します。

例

紐付け要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood association-request interval 100 threshold 100 quiet 360

2.1.67 flood authentication

Syntax

flood authentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood authentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 認証要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証要求フラッド攻撃アラームを引き起こす認証要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood authentication コマンドは認証要求フラッド攻撃検出を設定します。

undo flood authentication コマンドはデフォルトに戻します。

例

認証要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood authentication interval 100 threshold 100 quiet 360

2.1.68 flood beacon

Syntax

flood beacon [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood beacon

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ビーコンフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がビーコンフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にビーコンフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ビーコンフラッド攻撃アラームを引き起こすビーコンフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood beacon コマンドはビーコンフラッド攻撃検出を設定します。

undo flood beacon コマンドはデフォルトに戻します。

例

ビーコンフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood beacon interval 100 threshold 100 quiet 360

2.1.69 flood block-ack

Syntax

flood block-ack [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood block-ack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロックアクトフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロックアクトフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にブロックアクトフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロックアクトフラッド攻撃アラームを引き起こすブロックアクトフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood block-ack コマンドはブロックアクトフラッド攻撃検出を設定します。

undo flood block-ack コマンドはデフォルトに戻します。

例

ブロックアクトフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood block-ack interval 100 threshold 100 quiet 360

2.1.70 flood cts

Syntax

flood cts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood cts

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: CTS フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が CTS フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に CTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: CTS フラッド攻撃アラームを引き起こす CTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood cts コマンドは CTS フラッド攻撃検出を設定します。

undo flood cts コマンドはデフォルトに戻します。

例

CTS フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood cts interval 100 threshold 100 quiet 360

2.1.71 flood deauthentication

Syntax

flood deauthentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood deauthentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証取り消しフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証取り消しフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証取り消しフラッド攻撃アラームを引き起こす認証取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood deauthentication コマンドは認証取り消しフラッド攻撃検出を設定します。

undo flood deauthentication コマンドはデフォルトに戻します。

例

認証取り消しフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood deauthentication interval 100 threshold 100 quiet 360

2.1.72 flood disassociation

Syntax

flood disassociation [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood disassociation

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 紐付け取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が紐付け取り消しフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に紐付け取り消しフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 紐付け取り消しフラッド攻撃アラームを引き起こす紐付け取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood disassociation コマンドは紐付け取り消しフラッド攻撃検出を設定します。

undo flood disassociation コマンドはデフォルトに戻します。

例

紐付け取り消しフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood disassociation interval 100 threshold 100 quiet 360

2.1.73 flood eap-failure

Syntax

flood eap-failure [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-failure

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAP 失敗フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAP 失敗フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAP 失敗フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAP 失敗フラッド攻撃アラームを引き起こす EAP 失敗フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eap-failure コマンドは EAP 失敗フラッド攻撃検出を設定します。

undo flood eap-failure コマンドはデフォルトに戻します。

例

EAP 失敗フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood eap-failure interval 100 threshold 100 quiet 360

2.1.74 flood eapol-logoff

Syntax

flood eapol-logoff [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-logoff

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAPOL ログオフフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL ログオフフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL ログオフフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL ログオフフラッド攻撃アラームを引き起こす EAPOL ログオフフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-logoff コマンドは EAPOL ログオフフラッド攻撃検出を設定します。

undo flood eapol-logoff コマンドはデフォルトに戻します。

例

EAPOL ログオフフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood eapol-logoff interval 100 threshold 100 quiet 360

2.1.75 flood eapol-start

Syntax

flood eapol-start [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-start

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAPOL スタートフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL スタートフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL スタートフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL スタートフラッド攻撃アラームを引き起こす EAPOL スタートフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-start コマンドは EAPOL スタートフラッド攻撃検出を設定します。

undo flood eapol-start コマンドはデフォルトに戻します。

例

EAPOL スタートフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood eapol-start interval 100 threshold 100 quiet 360

2.1.76 flood eap-success

Syntax

flood eap-success [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-success

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAP 成功フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAP 成功フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAP 成功フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAP 成功フラッド攻撃アラームを引き起こす EAP 成功フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eap-success コマンドは EAP 成功フラッド攻撃検出を設定します。

undo flood eap-success コマンドはデフォルトに戻します。

例

EAP 成功フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood eap-success interval 100 threshold 100 quiet 360

2.1.77 flood null-data

Syntax

flood null-data [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood null-data

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ヌルデータフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がヌルデータフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にヌルデータフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ヌルデータフラッド攻撃アラームを引き起こすヌルデータフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood null-data コマンドはヌルデータフラッド攻撃検出を設定します。

undo flood null-data コマンドはデフォルトに戻します。

例

ヌルデータフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood null-data interval 100 threshold 100 quiet 360

2.1.78 flood probe-request

Syntax

flood probe-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood probe-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: プローブ要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がプローブ要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にプローブ要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: プローブ要求フラッド攻撃アラームを引き起こすプローブ要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood probe-request コマンドはプローブ要求フラッド攻撃検出を設定します。

undo flood probe-request コマンドはデフォルトに戻します。

例

プローブ要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood probe-request interval 100 threshold 100 quiet 360

2.1.79 flood reassociation-request

Syntax

flood reassociation-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood reassociation-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 再紐付け要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が再紐付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に再紐付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 再紐付け要求フラッド攻撃アラームを引き起こす再紐付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood reassociation-request コマンドは再紐付け要求フラッド攻撃検出を設定します。

undo flood reassociation-request コマンドはデフォルトに戻します。

例

再紐付け要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood reassociation-request interval 100 threshold 100 quiet 360

2.1.80 flood rts

Syntax

flood rts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood rts

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: RTS フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が RTS フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に RTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: RTS フラッド攻撃アラームを引き起こす RTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood rts コマンドは RTS フラッド攻撃検出を設定します。

undo flood rts コマンドはデフォルトに戻します。

例

RTS フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood rts interval 100 threshold 100 quiet 360

2.1.81 frame-type

Syntax

frame-type { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }

undo frame-type

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

control: 制御フレームと整合します。

data: データフレームと整合します。

management: 管理フレームと整合します。

frame-subtype: フレームサブタイプを指定します。

association-request: 紐付け要求フレームと整合します。

association-response: 紐付け応答フレームと整合します。

authentication: 認証フレームと整合します。

beacon: ビーコンフレームと整合します。

deauthentication: 認証取り消しフレームと整合します。

disassociation: 紐付け取り消しフレームと整合します。

probe-request: プローブ要求フレームと整合します。

説明

frame-type コマンドはフレームのフレームタイプと整合するためにサブ署名を設定します。

undo frame-type コマンドはデフォルトに戻します。

例

データフレームと一致するように signature 1 に対してサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] frame-type data

2.1.82 honeypot-ap

Syntax

honeypot-ap [**similarity** *similarity-value* | **quiet** *quiet-value*] *

undo honeypot-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

similarity *similarity-value*: ハニーポット AP アラームを引き起こす類似のしきい値を指定します。値の範囲は 70～100%です。デフォルト値は 80%です。AP の SSID と適合 AP の SSID との間の類似点がしきい値に達すると、AP はハニーポット AP とみなされます。

quiet *quiet-value*: WIPS がハニーポット AP 検出アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット AP を検出してもアラームを引き起こしません。

説明

honeypot-ap コマンドはハニーポット AP 検出を設定します。

undo honeypot-ap コマンドはハニーポット AP 検出を無効にします。

例

ハニーポット AP 検出を有効にします。類似のしきい値と遅延時間をそれぞれ、90%、10 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] honeypot-ap similarity 90 quiet 10

2.1.83 hotspot-attack

Syntax

hotspot-attack [**quiet** *quiet-value*]

undo hotspot-attack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がハニーポット攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット攻撃を検出してもアラームを引き起こしません。

説明

hotspot-attack コマンドはハニーポット攻撃検出を設定します。

undo hotspot-attack コマンドはハニーポット攻撃検出を無効にします。

例

ハニーポット攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] hotspot-attack quiet 100

2.1.84 hotspot ssid

Syntax

hotspot ssid *ssid-name*

undo hotspot ssid { *ssid-name* | **all** }

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

ssid-name: 名前で SSID を指定します。1 文字から 32 文字の文字列で、大文字と小文字が区別されます。

all: すべての SSID を指定します。

説明

hotspot ssid コマンドはホットスポット SSID として SSID を指定します。

undo hotspot ssid コマンドは指定された 1 つまたはすべてのホットスポット SSID を削除します。

デフォルトでは、装置にはホットスポット SSID が組み込まれています。組み込みのホットスポット SSID は削除できません。SSID をホットスポット SSID として指定するには、次のいずれかの操作を行います。

- 設定ファイルの SSID 設定を編集し、**import hotspot** コマンドを実行して、変更した設定ファイルを装置にインポートします。この方法を使用して、複数の SSID をホットスポット SSID として指定できます。
- **hotspot ssid** コマンドを実行して、ホットスポット SSID として SSID を指定します。

例

ホットスポット SSID に、SSID **cmcc** を指定します。

<AP> system-view

[AP] wips

[AP-wips] hotspot ssid cmcc

関連コマンド

import hotspot

2.1.85 ht-40mhz-intolerance

Syntax

ht-40mhz-intolerance [**quiet** *quiet-value*]

undo ht-greenfield

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が 40MHz の帯域幅モードを使用禁止にしたクライアントを検出するアラームを開始した後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を設定します。

undo ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を無効にします。

例

40MHz の帯域幅モードを使用禁止にしたクライアント検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ht-40mhz-intolerance quiet 100

2.1.86 ht-greenfield

Syntax

ht-greenfield [**quiet** *quiet-value*]

undo ht-greenfield

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が HT グリーンフィールド AP 検出アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-greenfield コマンドは HT グリーンフィールド検出を設定します。

undo ht-greenfield コマンドは HT グリーンフィールド検出を無効にします。

例

HT グリーンフィールド AP 検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ht-greenfield quiet 100

2.1.87 ignorelist

Syntax

ignorelist mac-address *mac-address*

undo ignorelist mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address: MAC アドレスを H-H-H 形式で指定します。

all: アラームを無視する装置リスト内のすべてのすべての MAC アドレスを指定します。

説明

ignorelist コマンドはアラームを無視する装置リストに MAC アドレスを追加します。

undo ignorelist コマンドはアラームを無視する装置リストから特定の、もしくはすべての MAC アドレスを削除します。

WIPS は、アラームを無視する装置リスト内の無線装置のみを監視しますが、アラームはあげません。

例

アラームを無視する装置リストに MAC アドレス **2a11-1fa1-1311** を追加します。

<AP> system-view

[AP] wips

[AP-wips] ignorelist mac-address 2a11-1fa1-1311

2.1.88 import hotspot

Syntax

import hotspot *file-name*

undo import hotspot

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import hotspot コマンドはコンフィグレーションファイルからホットスポットをインポートします。

undo import hotspot コマンドはコンフィグレーションファイルを削除します。

1 つのコンフィグレーションファイルからのみホットスポットをインポートできます。

例

コンフィグレーションファイル **hotspot_cfg** からホットスポットをインポートします。

<AP> system-view

[AP] wips

[AP-wips] import hotspot hotspot_cfg

2.1.89 import oui

Syntax

import oui *file-name*

undo import oui

デフォルト

インポートなし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import oui コマンドはコンフィグレーションファイルから OUI をインポートします。

undo import oui コマンドはコンフィグレーションを削除します。

IEEE ウェブサイトからコンフィグレーションファイルをダウンロードできます。

1 つのコンフィグレーションファイルからのみ OUI をインポートできます。

例

コンフィグレーションファイル **oui_import_cfg** から OUI をインポートします。

<AP> system-view

[AP] wips

[AP-wips] import oui oui_import_cfg

関連コマンド

invalid-oui-classify illegal

2.1.90 invalid-oui-classify illegal

Syntax

invalid-oui-classify illegal

undo invalid-oui-classify

デフォルト

無効

View

Classification policy view

定義済みユーザロール

network-admin

説明

invalid-oui-classify illegal コマンドは無効な OUI で装置を不正な装置として分類するように WIPS を有効にします

undo invalid-oui-classify コマンドはデフォルトに戻します。

例

無効な OUI で装置を不正な装置として分類するように WIPS を設定します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] invalid-oui-classify illegal

関連コマンド

import oui

2.1.91 mac-address

Syntax

mac-address { **bssid** | **destination** | **source** } *mac-address*

undo mac-address

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

bssid: 指定された BSSID と整合します。

destination: 指定された送信元 MAC アドレスと整合します。

source: 指定された送信元 MAC アドレスと整合します。

mac-address: MAC アドレスを H-H-H 形式で指定します。

説明

mac-address コマンドはフレームが送信元 MAC アドレスと整合するようにサブ署名を設定します。

undo mac-address コマンドはデフォルトに戻します。

例

フレームが送信元 MAC アドレス **000f-e201-0101** と整合するように signature 1 に対してサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] mac-address source 000f-e201-0101

2.1.92 malformed duplicated-ie

Syntax

malformed duplicated-ie [**quiet** *quiet-value*]

undo malformed duplicated-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が複製された IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に複製された IE を検出してもアラームを引き起こしません。

説明

malformed duplicated-ie コマンドは複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。

undo malformed duplicated-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。複製された IE をパケットが持つ場合、WIPS はパケットを異常とみなします。この検出はベンダに定義された IE には適用できません。

例

複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed duplicated-ie quiet 360

2.1.93 malformed fata-jack

Syntax

malformed fata-jack [**quiet** *quiet-value*]

undo malformed fata-jack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が FATA ジャック異常パケットアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に FATA ジャック異常パケットを検出してもアラームを引き起こしません。

説明

malformed fata-jack コマンドは FATA ジャック異常パケットを検出するように、WIPS を有効にします。

undo malformed fata-jack コマンドはデフォルトに戻します。

この機能は認証フレームに適用できます。認証アルゴリズム番号の値が 2 である場合、WIPS は認証フレームを異常とみなします。

例

複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed fata-jack quiet 360

2.1.94 malformed illegal-ibss-ess

Syntax

malformed illegal-ibss-ess [**quiet** *quiet-value*]

undo malformed illegal-ibss-ess

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常 IBSS および ESS 設定のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常 IBSS および ESS 設定を検出してもアラームを引き起こしません。

説明

malformed illegal-ibss-ess コマンドは異常 IBSS および ESS 設定をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed illegal-ibss-ess コマンドはデフォルトに戻します。

この機能はビーコンフレームおよびプローブ応答フレームに適用できます。IBSS と ESS がフレーム内でともに 1 に設定されている場合、WIPS はフレームを異常とみなします。

例

異常 IBSS および ESS 設定をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed illegal-ibss-ess quiet 360

2.1.95 malformed invalid-address-combination

Syntax

malformed invalid-address-combination [**quiet** *quiet-value*]

undo malformed invalid-address-combination

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な送信元アドレスのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な送信元アドレスを検出してもアラームを引き起こしません。

説明

malformed invalid-address-combination コマンドは無効な送信元アドレスをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-address-combination コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- フレームの TO DS が 1 の場合。（フレームがクライアントにより AP に送信されたことを示します）
- フレームの送信元 MAC アドレスがマルチキャストアドレスもしくはブロードキャストアドレスの場合。

例

無効な送信元アドレスをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-address-combination quiet 360

2.1.96 malformed invalid-assoc-req

Syntax

malformed invalid-assoc-req [**quiet** *quiet-value*]

undo malformed invalid-assoc-req

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常紐付け要求フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常紐付け要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-assoc-req コマンドは異常紐付け要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-assoc-req コマンドはデフォルトに戻します。

この機能は紐付け要求フレームに適用できます。フレーム内の SSID 長が 0 である場合、WIPS はフレームを異常とみなします。

例

異常紐付け要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-assoc-req quiet 360

2.1.97 malformed invalid-auth

Syntax

malformed invalid-auth [**quiet** *quiet-value*]

undo malformed invalid-auth

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常認証要求フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常認証要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-auth コマンドは異常認証要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-auth コマンドはデフォルトに戻します。

この機能は認証要求フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- 認証アルゴリズム番号が 802.11 プロトコルと一致せず、3 より大きい場合。
- 認証トランザクションシーケンス番号が 1 であり、状態コードが 0 で無い場合。（認証トランザクションシーケンス番号は、クライアントと AP 間の認証処理を示します。）
- 認証トランザクションシーケンス番号が 4 より大きい場合。

例

異常認証要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-auth quiet 360

2.1.98 malformed invalid-deauth-code

Syntax

malformed invalid-deauth-code [**quiet** *quiet-value*]

undo malformed invalid-deauth-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な認証取り消しコードのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な認証取り消しコードを検出してもアラームを引き起こしません。

説明

malformed invalid-deauth-code コマンドは無効な認証取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-deauth-code コマンドはデフォルトに戻します。

この機能は認証取り消しフレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを異常とみなします。

例

無効な認証取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-deauth-code quiet 360

2.1.99 malformed invalid-disassoc-code

Syntax

malformed invalid-disassoc-code [**quiet** *quiet-value*]

undo malformed invalid-disassoc-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な紐付け取り消しコードのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な紐付け取り消しコードを検出してもアラームを引き起こしません。

説明

malformed invalid-disassoc-code コマンドは無効な紐付け取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-disassoc-code コマンドはデフォルトに戻します。

この機能は紐付け取り消しフレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを異常とみなします。

例

無効な紐付け取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-disassoc-code quiet 360

2.1.100 malformed invalid-ht-ie

Syntax

malformed invalid-ht-ie [**quiet** *quiet-value*]

undo malformed invalid-ht-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常 HT IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常 HT IE を検出してもアラームを引き起こしません。

説明

malformed invalid-ht-ie コマンドは異常 HT IE をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ht-ie コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ応答フレーム、紐付け応答フレーム、再紐付け応答フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- HT ケーパビリティ IE の SM 電力節約値が 2 である場合。
- HT オペレーション IE のセカンダリチャネルオフセット値が 2 である場合。

例

異常 HT IE をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-ht-ie quiet 360

2.1.101 malformed invalid-ie-length

Syntax

malformed invalid-ie-length [**quiet** *quiet-value*]

undo malformed invalid-ie-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な IE 長のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な IE 長を検出してもアラームを引き起こしません。

説明

malformed invalid-ie-length コマンドは無効な IE 長をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ie-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE 長が 802.11 プロトコルと一致しない場合、WIPS はフレームを異常とみなします。

例

無効な IE 長をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-ie-length quiet 360

2.1.102 malformed invalid-pkt-length

Syntax

malformed invalid-pkt-length [**quiet** *quiet-value*]

undo malformed invalid-pkt-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効なパケット長のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効なパケット長を検出してもアラームを引き起こしません。

説明

malformed invalid-pkt-length コマンドは無効なパケット長をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-pkt-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。パケットペイロード解析後に IE の残存長が 0 で無い場合、WIPS はフレームを異常とみなします。

例

無効なパケット長をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-pkt-length quiet 360

2.1.103 malformed large-duration

Syntax

malformed large-duration [**quiet** *quiet-value* | **threshold** *value*]

undo malformed large-duration

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな期間のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな期間を検出してもアラームを引き起こしません。

threshold *threshold-value*: WIPS がオーバーサイズな期間を判断し、アラームをあげるために、期間のサイズを指定します。*value* 引数の値の範囲は 1～32767 です。デフォルト値は 5000 です。

説明

malformed large-duration コマンドはオーバーサイズな期間をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed large-duration コマンドはデフォルトに戻します。

この機能はユニキャスト管理フレーム、ユニキャストデータフレーム、RTS フレーム、CTS フレーム、ACK フレームに適用できます。フレーム内の期間の値が指定されたしきい値より大きい場合、WIPS はフレームを異常とみなします。

例

オーバーサイズな期間をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed large-duration quiet 360

2.1.104 malformed null-probe-resp

Syntax

malformed null-probe-resp [**quiet** *quiet-value*]

undo malformed null-probe-resp

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常プローブ応答フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常プローブ応答フレームを検出してもアラームを引き起こしません。

説明

malformed null-probe-resp コマンドは異常プローブ応答フレームを検出するように、WIPS を有効にします。

undo malformed null-probe-resp コマンドはデフォルトに戻します。

この機能はプローブ応答フレームに適用できます。フレームがメッシュフレームでなく、SSID 長が 0 である場合、WIPS はフレームを異常とみなし、パケットは異常パケットとみなします。

例

異常プローブ応答フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed null-probe-resp quiet 360

2.1.105 malformed overflow-eapol-key

Syntax

malformed overflow-eapol-key [**quiet** *quiet-value*]

undo malformed overflow-eapol-key

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな EAPOL 鍵のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな EAPOL 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-eapol-key コマンドはオーバーサイズな EAPOL 鍵をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed overflow-eapol-key コマンドはデフォルトに戻します。

この機能は EAPOL 鍵フレームに適用できます。フレーム内の TO DS が 1 で、鍵長が 0 より大きい場合、WIPS はフレームを異常とみなします。悪意ある EAPOL 鍵フレームにより DOS 攻撃を受ける恐れがあります。

例

オーバーサイズな EAPOL 鍵をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed overflow-eapol-key quiet 360

2.1.106 malformed overflow-ssid

Syntax

malformed overflow-ssid [**quiet** *quiet-value*]

undo malformed overflow-ssid

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな SSID のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな SSID 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-ssid コマンドはオーバーサイズな SSID をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed overflow-ssid コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ要求フレーム、プローブ応答フレーム、紐付け要求フレームに適用できます。フレーム内の SSID 長が 32 より大きく、802.11 プロトコルに一致していない場合、WIPS はフレームを異常とみなします。

例

オーバーサイズな SSID をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed overflow-ssid quiet 360

2.1.107 malformed redundant-ie

Syntax

malformed redundant-ie [**quiet** *quiet-value*]

undo malformed redundant-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が冗長な IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に冗長な IE を検出してもアラームを引き起こしません。

説明

malformed redundant-ie コマンドは冗長な IE をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed redundant-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE がフレームにとって必要な IE でも予備の IE でもない場合、WIPS はフレームを異常とみなします。

例

冗長な IE をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed redundant-ie quiet 360

2.1.108 man-in-the-middle

Syntax

man-in-the-middle [**quiet** *quiet-value*]

undo man-in-the-middle

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が MITM（Man-In-The-Middle）攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に MITM 攻撃を検出してもアラームを引き起こしません。

説明

man-in-the-middle コマンドは MITM 攻撃検出を有効にします。

undo man-in-the-middle コマンドは MITM 攻撃検出を無効にします。

MITM 攻撃検出を有効にする前にハニーポット AP 検出を有効にしてください。

例

MITM 攻撃検出を有効にします。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] honeypot-ap

[AP-wips-dtc-home] man-in-the-middle

2.1.109 manual-classify mac-address

Syntax

manual-classify mac-address *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }

undo manual-classify mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを H-H-H 形式で指定します。

authorized-ap: AP を許可された AP として指定します。

external-ap: AP を外部 AP として指定します。

misconfigured-ap: AP を間違って設定された AP として指定します。

rogue-ap: AP を不正な AP として指定します。

all: すべての AP を指定します。

説明

manual-classify mac-address コマンドは AP に対してカテゴリを設定します。

undo manual-classify mac-address コマンドはデフォルトに戻します。

例

MAC アドレスが 000f-00e2-0001 の AP を許可された AP として設定します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] manual-classify mac-address 000f-00e2-0001 authorized-ap

2.1.110 match all (AP classification rule view)

Syntax

match all

undo match all

デフォルト

AP 分類ルールの基準は、論理 OR 関係にあります。AP 分類ルールの基準のいずれかに一致する場合、AP は AP 分類ルールに一致します。

View

AP classification rule view

定義済みユーザロール

network-admin

説明

match all コマンドは AP 分類ルールの基準が論理 AND 関係になるように設定します。

undo match all コマンドはデフォルトに戻します。

例

AP 分類ルール 1 の基準を論理 AND 関係にするように設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] match all

2.1.111 match all (signature view)

yntax

match all

undo match all

デフォルト

副署名は論理 OR 関係にあります。パケットは、署名のいずれかの副署名と一致する場合、署名と一致します。

View

Signature view

定義済みユーザロール

network-admin

説明

match all コマンドはサブ署名が論理 AND 関係になるように設定します。

undo match all コマンドはデフォルトに戻します。

例

署名 1 の副署名を論理 AND 関係にするように設定します

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[wips-sig-rule-1] match all

関連コマンド

- **frame-type**
- **mac-address**
- **pattern**
- **seq-number**
- **ssid (signature rule view)**
- **ssid-length**

2.1.112 omerta

Syntax

omerta [**quiet** *quiet-value*]

undo omerta

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Omerta 攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に Omerta 攻撃を検出してもアラームを引き起こしません。

説明

omerta コマンドは Omerta 攻撃検出を有効にします。

undo omerta コマンドは Omerta 攻撃検出を無効にします。

例

Omerta 攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] omerta quiet 100

2.1.113 oui

Syntax

oui *oui-info*

undo oui

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

oui-info: OUI 情報を XXXXXX 形式で指定します。大文字と小文字を区別しません。16 進数で指定します。

説明

oui コマンドは AP の OUI 情報と整合するように AP 分類ルールを設定します。

undo oui コマンドはデフォルトに戻します。

例

AP を OUI **000fe4** と整合するために AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] oui 000fe4

2.1.114 pattern

Syntax

pattern *pattern-number* **offset** *offset-value* **mask** *mask value1* [**to** *value2*] [**from-payload**]

undo pattern { *pattern-number* | **all** }

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

pattern-number: 0〜65535 の範囲の数字で指定されたフレームのビットと一致するサブ署名を指定します。

offset *offset-value*: 指定されたビットから参照ビットまでのオフセットを指定します。*offset-value* 引数の値の範囲は 0〜2346 ビットです。参照ビットは、フレームヘッド（デフォルト）もしくはフレームペイロードの最初のビットになることができます。

mask *mask*: 指定されたビットで AND 演算に使用される 2 バイトマスクを指定します。マスクは 16 進数形式です。マスクの値の範囲は 0〜ffff です。

value1 [**to** *value2*]: ビット数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0〜65535 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

from-payload: 参照ビットとしてフレームペイロードの最初のビットを指定します。このキーワードを指定しない場合、フレームヘッドの最初のビットは参照ビットになります。

説明

pattern コマンドは指定されたフレームのビットと整合するようにサブ署名を設定します。

undo pattern コマンドはデフォルトに戻します。

例

フレームヘッドの第 2 ビットと第 3 ビットが整合するようにサブ署名を設定します。フレームの第 2 ビットと第 3 ビットの値が 0x0015〜0x0020 の範囲内の場合、フレームはサブ署名と整合します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] pattern 1 offset 8 mask ffff 15 to 20

2.1.115 permit-channel

Syntax

permit-channel *channel-id-list*

undo permit-channel { *channel-id-list* | **all** }

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

channel-id-list: 許可された 10 個までのチャネルアイテムの空間分離リストを指定します。各アイテムは、*value1* **to** *value2* の形式でチャネル番号もしくはチャネル番号の範囲を指定します。チャネル番号の範囲は 1～224 です。*value2* 引数の値は *value1* 引数の値以上でなければなりません。

all: 許可されたすべてのチャネルを指定します。

説明

permit-channel コマンドは許可されたチャネルリストに 1 つあるいは複数のチャネルを追加します。

undo permit-channel コマンドは許可されたチャネルリストから指定されたチャネルあるいはすべてのチャネルを削除します。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、このコマンドを使用して許可されたチャネルリストを設定します。

例

チャネル 1 を許可されたチャネルリストに追加します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] permit-channel 1

関連コマンド

prohibited-channel

2.1.116 power-save

Syntax

power-save [**interval** *interval-value* | **minoffpacket** *packet-value* | **onoffpercent** *percent-value* | **quiet** *quiet-value*] *

undo power-save

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: パワーセーブフレームのための統計値収集間隔を指定します。*interval-value* 引数の値は 1～3600 秒です。デフォルト値は 10 秒です。

minoffpacket *packet-value*: パワーセーブ攻撃分析を引き起こすパワーセーブ off フレームの数のしきい値を指定します。クライアントからの off フレームの数がしきい値の達すると、WIPS はパワーセーブ攻撃が発生したかどうか判断するために、パワーセーブフレームを分析します。値の範囲は 10～150 です。デフォルト値は 50 です。

onoffpercent *percent-value*: クライアントからのパワーセーブ on フレームと off フレームの比率のしきい値を指定します。しきい値に達すると WIPS はパワーセーブ攻撃のアラームを引き起こします。値の範囲は 0～100 です。デフォルト値は 80 です。

quiet *quiet-value*: WIPS がパワーセーブ攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にパワーセーブ攻撃を検出してもアラームを引き起こしません。

説明

power-save コマンドはパワーセーブ攻撃検出を有効にします。

undo power-save コマンドはパワーセーブ攻撃検出を無効にします。

例

パワーセーブ攻撃検出を有効にします。*interval-value*、*packet-value*、*percent-value*、*quiet-value* の値をそれぞれ、20、20、90、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] power-save interval 20 minoffpacket 20 onoffpercent 90 quiet 100

2.1.117 prohibited-channel

Syntax

prohibited-channel [**quiet** *quiet-value*]

undo prohibited-channel

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が禁止されたチャネルのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に禁止されたチャネルを検出してもアラームを引き起こしません。

説明

prohibited-channel コマンドは禁止されたチャネル検出を有効にします。

undo prohibited-channel コマンドは禁止されたチャネル検出を無効にします。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、**permit-channel** コマンドを使用して許可されたチャネルリストを設定します。

例

禁止されたチャネル検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] prohibited-channel quiet 100

関連コマンド

permit-channel

2.1.118 random-mac-scan

Syntax

random-mac-scan enable

undo random-mac-scan enable

デフォルト

WIPS は、ランダムな MAC アドレスを使用する Apple 端末のアラームをトリガーします。

View

Attack detection policy view

定義済みユーザロール

network-admin

説明

random-mac-scan enable コマンドはランダムな MAC アドレスを使用する Apple 端末のアラームをトリガーしないように WIPS を設定します。

undo random-mac-scan enable コマンドはデフォルトに戻します。

例

ランダムな MAC アドレスを使用する Apple 端末のアラームをトリガーしないように WIPS を設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] random-mac-scan enable

2.1.119 report-interval

Syntax

report-interval *interval*

undo report-interval

デフォルト

AP は、検出されたデバイスに関する情報を 30000 ミリ秒ごとに報告します。

View

User view

定義済みユーザロール

network-admin

パラメータ

interval: 検出されたデバイスに関する情報を AP がレポートする間隔を 1000~300000 ミリ秒の範囲で指定します。

説明

report-interval コマンドは検出されたデバイスに関する情報を AP が報告する間隔を設定します。

undo report-interval コマンドはデフォルトに戻します。

例

検出されたデバイスに関する情報を AP が報告する間隔を 10000 ミリ秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] report-interval 10000

2.1.120 reset wips embedded-oui

Syntax

reset wips embedded-oui

View

User view

定義済みユーザロール

network-admin

説明

report-interval コマンドは、OUI ライブラリ内のすべての埋め込み OUI を削除します。

例

OUI ライブラリの埋め込み OUI をすべて削除します。

<AP> reset wips embedded-oui

関連コマンド

- **export oui**
- **import oui**

2.1.121 reset wips statistics

Syntax

reset wips statistics

View

User view

定義済みユーザロール

network-admin

説明

reset wips statistics コマンドはすべてのセンサから収集した情報を消去します。

例

すべてのセンサから収集した情報を消去します。

<AP> reset wips statistics

関連コマンド

display wips statistics receive

2.1.122 reset wips virtual-security-domain

Syntax

reset wips virtual-security-domain *vsd-name* **device** { **ap** { **all** | **mac-address** *mac-address* } | **client** { **all** | **mac-address** *mac-address* } | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 装置のエントリを消去します。

ap: AP のエントリを消去します。

all: すべての AP のエントリを消去します。

mac-address *mac-address*: AP のエントリを消去します。*mac-address* 引数は AP の MAC アドレスをあらわします。

client: クライアントのエントリを消去します。

all: すべてのクライアントのエントリを消去します。

mac-address *mac-address*: クライアントのエントリを消去します。*mac-address* 引数はクライアントの MAC アドレスをあらわします。

all: すべての AP とクライアントのエントリを消去します。

説明

reset wips virtual-security-domain コマンドは VSD にある学習した AP もしくはクライアントのエントリを消去します。

例

VSD **aaa** にある学習した AP とクライアントのエントリを消去します。

<AP> reset wips virtual-security-domain aaa device all

関連コマンド

display wips virtual-security-domain device

2.1.123 reset wips virtual-security-domain countermeasure record

Syntax

reset wips virtual-security-domain *vsd-name* **countermeasure record**

View

User view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

reset wips virtual-security-domain countermeasure record コマンドは WIPS が不正な装置に対して講じた対策に関する情報を消去します。

例

VSD **aaa** のために WIPS が不正な装置に対して講じた対策に関する情報を消去します。

<AP> reset wips virtual-security-domain aaa countermeasure record

関連コマンド

display wips virtual-security-domain countermeasure record

2.1.124 rssi-change-threshold

Syntax

rssi-change-threshold *threshold-value*

undo rssi-change-threshold

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

threshold-value: ワイヤレス装置検出の RSSI 差分しきい値を 1~100 の範囲で指定します。。

説明

rssi-change-threshold コマンドは AP の RSSI と整合するように AP 分類ルールを設定します。

undo rssi-change-threshold コマンドはデフォルトに戻します。

例

ワイヤレス装置検出の RSSI 差分しきい値を 80 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] rssi-change-threshold 80

2.1.125 rssi-threshold

Syntax

rssi-threshold { **ap** *ap-rssi-value* | **client** *client-rssi-value* }

undo rssi-threshold { **ap** | **client** }

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

ap *ap-rssi-value* :AP の RSSI しきい値を 1~100 の範囲で指定します。

client *client-rssi-value*: クライアントの RSSI しきい値を 1~100 の範囲で指定します。

説明

rssi-threshold コマンドはクライアントまたは AP の RSSI しきい値を設定します。

undo rssi-threshold コマンドはデフォルトに戻します。

例

AP の RSSI しきい値を 80 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] rssi-threshold ap 80

2.1.126 rssi

Syntax

rssi *value1* [**to** *value2*]

undo rssi

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 [**to** *value2*]: AP の RSSI の値の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～100 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

rssi コマンドは AP の RSSI と整合するように AP 分類ルールを設定します。

undo rssi コマンドはデフォルトに戻します。

例

AP が 20～40 の RSSI と整合するように AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] rssi 20 to 40

2.1.127 security

Syntax

security { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }

undo security

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

equal: 指定されたセキュリティモードと等しいセキュリティモードと整合します。

include: 指定されたセキュリティモードを含むセキュリティモードと整合します。

clear: 消去するセキュリティモードを指定します。

wep: WEP セキュリティモードを指定します。

wpa: WPA セキュリティモードを指定します。

wpa2: WPA2 セキュリティモードを指定します。

説明

security コマンドは AP に使用されるセキュリティモードと整合するように AP 分類ルールを設定します。

undo security コマンドはデフォルトに戻します。

例

WEP セキュリティモードを使用する AP と整合するように AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] security equal wep

2.1.128 select sensor all

Syntax

select sensor all

undo select sensor all

デフォルト

直近で攻撃者を検出したセンサのみ、その攻撃者に対して対策を講じます。

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

select sensor all コマンドは攻撃者を検出するすべてのセンサを有効にします。

undo select sensor all コマンドは設定を削除します。

例

攻撃者に対して対策を講じるために、攻撃者を検出するすべてのセンサを有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-ctm-home] select sensor all

2.1.129 seq-number

Syntax

seq-number *seq-value1* [**to** *seq-value2*]

undo seq-number

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

seq-value1 [**to** *seq-value2*]: フレームのシーケンス番号の範囲を指定します。*seq-value1* 引数と *seq-value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*seq-value 1* 引数と *seq-value 2* 引数の値の範囲は、どちらも 0～4095 です。ただし、*seq-value 2* 引数の値は *seq-value 1* 引数の値より大きくなければなりません。

説明

seq-number コマンドはシーケンス番号をもつフレームと整合するサブ署名を設定します。

undo seq-number コマンドはデフォルトに戻します。

例

シーケンス番号 100 をもつフレームと整合するサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] seq-number 100

2.1.130 signature policy

Syntax

signature policy *policy-name*

undo signature policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 署名ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

signature policy コマンドは署名ポリシーを作成し、その view に移行します。指定された署名ポリシーがすでに存在する場合、signature policy view に移行します。

undo signature policy コマンドは署名ポリシーを削除します。

例

署名ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] signature policy home

2.1.131 signature rule

Syntax

signature rule *rule-id*

undo signature rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

rule-id: 署名の ID を指定します。範囲は 1～65535 です。

説明

signature rule コマンドは署名を作成し、その view に移行します。指定された署名がすでに存在する場合、signature view に移行します。

undo signature rule コマンドは署名を削除します。

例

signature 1 を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

2.1.132 soft-ap

Syntax

soft-ap [**convert-time** *time-value*]

undo soft-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

convert-time *time-value*: ソフト AP がクライアントと AP の役割を切り替える間隔を指定します。*time-value* 引数の値の範囲は 5〜600 秒です。デフォルト値は 10 秒です。

説明

soft-ap コマンドはソフト AP 検出を有効にします。

undo soft-ap コマンドはソフト AP 検出を無効にします。

例

ソフト AP 検出を有効にします。*time-value* 引数の値を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] soft-ap convert-time 100

2.1.133 ssid (AP classification rule view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*

undo ssid

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

ssid-string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドは AP に対して無線装置の SSID を整合するように AP 分類ルールを設定します。

undo ssid コマンドはデフォルトに戻します。

例

SSID **abc** の無線サービスを使用した AP を整合するために AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] ssid equal abc

2.1.134 ssid (signature view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *string*

undo ssid

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドはフレームの SSID を整合するためにサブ署名を設定します。

undo ssid コマンドはデフォルトに戻します。

例

signature 1 に対して SSID **office** のフレームを整合するためにサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] ssid equal office

2.1.135 ssid-length

Syntax

ssid-length *length-value1* [**to** *length-value2*]

undo ssid-length

デフォルト

設定なし

View

Signature rule

定義済みユーザロール

network-admin

パラメータ

length-value1 [**to** *length-value2*]: SSID 長の値の範囲を指定します。*length-value1* 引数と *length-value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*length-value 1* 引数と *length-value 2* 引数の値の範囲は、どちらも 1～32 です。ただし、*length-value 2* 引数の値は *length-value 1* 引数の値より大きくなければなりません。

説明

ssid-length コマンドはフレームの SSID 長を整合するためにサブ署名を設定します。

undo ssid-length コマンドはデフォルトに戻します。

例

SSID 長が 10 のフレームを整合するためにサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-1] ssid-length 10

2.1.136 trust mac-address

Syntax

trust mac-address *mac-address*

undo trust mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: MAC アドレスを指定します。

all: すべての MAC アドレスを指定します。

説明

trust mac-address コマンドは許可された装置リストに AP もしくはクライアントの MAC アドレスを追加します。

undo trust mac-address コマンドは許可された装置リストから 1 つあるいはすべての MAC アドレスを削除します。

例

許可された装置リストに MAC アドレス **78AC-C0AF-944F** を追加します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] trust mac-address 78AC-C0AF-944F

2.1.137 trust oui

Syntax

trust oui *oui*

undo trust oui { *oui* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

oui: OUI の名前を指定します。大文字と小文字を区別しません。文字数は 6 文字です。

all: すべての OUI を指定します。

説明

trust oui コマンドは信頼された OUI リストに OUI を追加します。

undo trust oui コマンドは信頼された OUI リストから 1 つあるいはすべての OUI を削除します。

例

信頼された OUI リストに OUI **000fe4** と **000fe5** を追加します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] trust oui 000fe4

[AP-wips-cls-home] trust oui 000fe5

2.1.138 trust ssid

Syntax

trust ssid *ssid-name*

undo trust ssid { *ssid-name* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID の名前を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

all: すべての SSID を指定します。

説明

trust ssid コマンドは信頼された SSID リストに SSID を追加します。

undo trust ssid コマンドは信頼された SSID リストから 1 つあるいはすべての SSID を削除します。

例

信頼された SSID リストに SSID **flood1** を追加します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] trust ssid flood1

2.1.139 unencrypted-authorized-ap

Syntax

unencrypted-authorized-ap [**quiet** *quiet-value*]

undo unencrypted-authorized-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可 AP を検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可 AP を検出してもアラームを引き起こしません。

説明

unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を有効にします。

undo unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を無効にします。

例

暗号化されていない許可 AP 検出を有効にします。遅延時間を 10 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] unencrypted-authorized-ap quiet 10

2.1.140 unencrypted-trust-client

Syntax

unencrypted-trust-client [**quiet** *quiet-value*]

undo unencrypted-trust-client

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可クライアントを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可クライアントを検出してもアラームを引き起こしません。

説明

unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を有効にします。

undo unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を無効にします。

例

暗号化されていない許可クライアント検出を有効にします。遅延時間を 10 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] unencrypted-trust-client quiet 10

2.1.141 up-duration

Syntax

up-duration *value1* [**to** *value2*]

undo up-duration

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 [**to** *value2*]: AP の動作時間の値の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～2592000 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

up-duration コマンドを使用して、AP の動作時間と整合するように AP 分類ルールを設定します。

undo up-duration コマンドでデフォルトに戻します。

例

2000～40000 秒の動作時間の AP と整合するように AP 分類ルールを設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] up-duration 2000 to 40000

2.1.142 virtual-security-domain

Syntax

virtual-security-domain *vsd-name*

undo virtual-security-domain *vsd-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

virtual-security-domain コマンドは VSD を作成し、その view に移行します。

undo virtual-security-domain コマンドは VSD を削除します。

例

VSD **office** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain office

[AP-wips-vsd-office]

2.1.143 weak-iv

Syntax

weak-iv [**quiet** *quiet-value*]

undo weak-iv

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がウィーク IV のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にウィーク IV を検出してもアラームを引き起こしません。

説明

weak-iv コマンドはウィーク IV 検出を有効にします。

undo weak-iv コマンドはデフォルトに戻します。

例

ウィーク IV 検出を有効にします。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] weak-iv

2.1.144 windows-bridge

Syntax

windows-bridge [**quiet** *quiet-value*]

undo windows-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Windows ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に Windows ブリッジを検出してもアラームを引き起こしません。

説明

windows-bridge コマンドは Windows ブリッジ検出を有効にします。

undo wireless-bridge コマンドは Windows ブリッジを無効にします。

例

Windows ブリッジ検出を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] windows-bridge quiet 360

2.1.145 wips(system view)

Syntax

wips

undo wips

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

説明

wips コマンドは WIPS view に移行します。

undo wips コマンドは WIPS view 内の設定をすべて削除します。

例

WIPS view に移行します。

<AP> system-view

[AP] wips

[AP-wips]

2.1.146 wips(radio view)

Syntax

wips { disable | enable }

undo wips

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: WIPS を無効にします。

enable: WIPS を有効にします。

説明

wips enable コマンドは WIPS を有効にします。

wips disable コマンドは WIPS を無効にします。

undo wips コマンドはデフォルトに戻します。

例

WLAN-radio 1/0/1 の WIPS を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1] wips enable

2.1.147 wips virtual-security-domain

Syntax

wips virtual-security-domain *vsd-name*

undo wips virtual-security-domain

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、AP グループは VSD に追加されません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

wips virtual-security-domain コマンドは AP を VSD に追加します。

undo wips virtual-security-domain コマンドは AP を VSD から削除します。

例

AP group **apgroup1** を VSD **office** に追加します。

<AP> system-view

[AP] wlan ap-group apgroup1

[AP-wlan-ap-group-apgroup1] wips virtual-security-domain office

2.1.148 wireless-bridge

Syntax

wireless-bridge [**quiet** *quiet-value*]

undo wireless-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無線ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に無線ブリッジを検出してもアラームを引き起こしません。

説明

wireless-bridge コマンドは無線ブリッジ検出を有効にします。

undo wireless-bridge コマンドは無線ブリッジを無効にします。

例

無線ブリッジ検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] wireless-bridge quiet 100

QX-W610 アクセスポイント

コマンドマニュアル

08.WLAN セキュリティ

本マニュアルは以下に示す章で構成されています。

01-WLAN セキュリティ

02-WIPS

目次

このセクションのページは **8-x-x** です。

1 章 WLAN セキュリティ 1-1
1.1 WLAN セキュリティの設定コマンド 1-1
1.1.1 akm mode 1-1
1.1.2 akm sae pwe 1-2
1.1.3 cipher-suite 1-3
1.1.4 enhanced-open enable 1-4
1.1.5 enhanced-open transition-mode service-template 1-6
1.1.6 gtk-rekey client-offline enable 1-7
1.1.7 gtk-rekey enable 1-8
1.1.8 gtk-rekey method 1-8
1.1.9 key-derivation 1-10
1.1.10 pmf 1-11
1.1.11 pmf association-comeback 1-12
1.1.12 pmf saquery retrycount 1-13
1.1.13 pmf saquery retrytimeout 1-14
1.1.14 preshared-key 1-15
1.1.15 ptk-lifetime 1-16
1.1.16 ptk-rekey enable 1-17
1.1.17 security-ie 1-18
1.1.18 snmp-agent trap enable wlan usersec 1-19
1.1.19 tkip-cm-time 1-19
1.1.20 wlan password-failure-limit enable 1-21
1.1.21 wpa3 1-22

1章 WLAN セキュリティ

1.1 WLANセキュリティの設定コマンド

1.1.1 akm mode

Syntax

akm mode { **dot1x** | **psk** }

undo akm mode

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

dot1x: 802.1X を指定します。

psk: PSK を指定します。

説明

akm mode コマンドは AKM（Authentication and Key Management）モードを設定します。

undo akm mode コマンドはデフォルトに戻します。

RSNA ネットワークに AKM モードを設定する必要があります。

WLAN サービステンプレートは AKM モードを 1 つだけサポートします。WLAN サービステンプレートが無効なときだけ AKM モードを設定します。

以下の AKM モードは、いずれも特定の認証モードで使用する必要があります。

- **802.1X AKM—**802.1X 認証モード
- **PSK AKM—**MAC もしくは認証バイパスモード

詳細は、オペレーションマニュアルのセクション 5 *WLAN アクセス “WLAN アクセスの設定”* を参照してください。

例

PSK AKM モードを設定します。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] akm mode psk

関連コマンド

- **cipher-suite**
- **security-ie**

1.1.2 akm sae pwe

メモ：

- **akm sae pwe** コマンドは v7.5.105 を含む以降のソフトウェアからサポートしています。
- **both-h2e-hnp** を指定すると、**hnp** のみをサポートしたクライアントでローミングに失敗する場合があります。クライアントの問題ですが、ローミング失敗を避けるためには、”**akm sae pwe hnp**” を設定してください。

Syntax

akm sae pwe { **both-h2e-hnp** | **h2e** | **hnp** }

undo akm sae pwe { **both-h2e-hnp** | **h2e** | **hnp** }

デフォルト

both-h2e-hnp

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

both-h2e-hnp：PWE の生成方式として、Hunting-and-Pecking (HnP) と Hash-to-Element (H2E) を指定します。

h2e：PWE の生成方式として、Hash-to-Element (H2E) を指定します。

hnp：PWE の生成方式として、Hunting-and-Pecking (HnP) を指定します。

説明

akm sae pwe コマンドは WPA3-SAE の SAE 交換時の PWE 生成方式を設定します。**undo akm sae pwe** コマンドはこの設定をデフォルト (both-h2e-hnp) に戻します。WPA3-SAE では、Hunting-and-Pecking (HnP) と Hash-to-Element (H2E) の両方の方法で PWE の生成が可能です。H2E は最新の PWE 生成方法であり、強化されたセキュリティパフォーマンスを提供します。

もし、クライアントが指定された PWE 生成方式をサポートしていない場合、そのクライアントは無線ネットワークにアクセスできません。クライアントの互換性を向上させる場合は、**both-h2e-hnp** を指定してください。

例

WPA3-SAE の PWE 生成方式として H2E を設定します。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] akm sae pwe h2e

WPA3-SAE の設定を確認するには、**display wlan service-template** コマンドを実行します。

<AP> display wlan service-template security verbose | include SAE

SAE PWE method :Hash-to-Element(H2E)

関連コマンド

display wlan service-template

1.1.3 cipher-suite

Syntax

cipher-suite { **ccmp** | **gcmp** | **tkip** }

undo cipher-suite { **ccmp** | **gcmp** | **tkip** }

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

ccmp: AES-CCMP 暗号方式を指定します。

gcmp: AES-GCMP 暗号方式を指定します。

tkip: TKIP 暗号方式を指定します。

説明

cipher-suite コマンドはフレーム暗号化に使用する暗号方式を指定します。

undo cipher-suite コマンドは指定した暗号方式を無効にします。

RSNA ネットワークに暗号方式を指定しなければなりません。WLAN サービステンプレートが無効の場合のみ暗号方式を設定します。

RSN IE あるいは WPA IE を設定するとき、TKIP、CCMP、あるいは GCMP 暗号方式を設定します。

例

TKIP 暗号方式を設定します。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] cipher-suite tkip

関連コマンド

security-ie

1.1.4 enhanced-open enable

Syntax

enhanced-open enable

undo enhanced-open enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

enhanced-open enable コマンドは Enhanced Open システム認証を有効にします。

undo enhanced-open enable コマンドは Enhanced Open システム認証を無効にします。

例

Enhanced Open システム認証を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] enhanced-open enable

関連コマンド

enhanced-open transition-mode service-template

1.1.5 enhanced-open transition-mode service-template

Syntax

enhanced-open transition-mode service-template *service-template-name*

undo enhanced-open transition-mode service-template

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

service-template-name: 大文字と小文字を区別しない 1～63 文字の文字列でサービステンプレートの名前を指定します。

説明

enhanced-open transition-mode service-template コマンドは移行モードでの推奨サービステンプレートを指定します。

undo enhanced-open transition-mode service-template コマンドはデフォルト設定に戻します。

このコマンドを複数回実行した場合、最後に実行した設定が反映されます。

例

サービステンプレート **service1** に対して、移行モードでの推奨サービステンプレートとして **service2** を指定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] enhanced-open transition-mode service-template service2

関連コマンド

- **beacon ssid-hide**
- **enhanced-open enable**

1.1.6 gtk-rekey client-offline enable

Syntax

gtk-rekey client-offline enable

undo gtk-rekey client-offline enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

gtk-rekey client-offline enable コマンドは offline-triggered GTK update を有効にします。

undo gtk-rekey client-offline コマンドはデフォルトに戻します。

GTK update が有効な場合のみ offline-triggered GTK update を有効にします。

例

offline-triggered GTK update を有効にします。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] gtk-rekey client-offline enable

関連コマンド

gtk-rekey enable

1.1.7 gtk-rekey enable

Syntax

gtk-rekey enable

undo gtk-rekey enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

gtk-rekey enable コマンドは GTK update を有効にします。

undo gtk-rekey enable コマンドは GTK update を無効にします。

例

GTK update を有効にします。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] gtk-rekey enable

1.1.8 gtk-rekey method

Syntax

gtk-rekey method { **packet-based** [*packet*] | **time-based** [*time*] }

undo gtk-rekey method

デフォルト

GTK は 86400 秒間隔でアップデートされます。

伝送パケット数のデフォルトは 10000000 です。

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

packet-based *packet*: GTK がアップデートされる前に、マルチキャストとブロードキャストを含む伝送パケットの数を指定します。設定範囲は 5000～4294967295 です。

time-based *time*: GTK がアップデートされる間隔を指定します。設定範囲は 180～604800 秒です。

説明

gtk-rekey method コマンドは GTK update 手法を設定します。

undo gtk-rekey method コマンドはデフォルトに戻します。

GTK update が有効な場合のみ GTK update 手法を設定します。

直近のコンフィグレーションは、それ以前のコンフィグレーションを上書きします。例えば、packet に基づく手法を設定した後 time に基づく設定をする場合、time に基づく手法が適用されます。

サービステンプレートが有効になった後 GTK update 手法を設定する場合、以下の条件が存在するとき変更点が反映されます。

- GTK update 間隔を変更する場合、すでに設定されていたタイマが終了したとき新たな間隔が反映されます。
- パケット数のしきい値を変更する場合、新たなしきい値は即座に反映されます。
- GTK update 手法を packet に基づく設定に変更する場合、タイマが消去されパケット数がしきい値に達したとき新たな設定が反映されます。
- GTK update 手法を time に基づく設定に変更する場合、新たな設定は即座に反映されます。

例

アップデート間隔に基づく GTK update を有効にします。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] gtk-rekey method time-based 3600

パケットに基づく GTK update を有効にします。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] gtk-rekey method packet-based 600000

関連コマンド

gtk-rekey enable

1.1.9 key-derivation

Syntax

key-derivation { **sha1** | **sha1-and-sha256** | **sha256** }

undo key-derivation

デフォルト

sha1

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

sha1: HMAC-SHA1 アルゴリズムを指定します。

sha256: HMAC-SHA256 アルゴリズムを指定します。

sha1-and-sha256: HMAC-SHA1 アルゴリズムと HMAC-SHA256 アルゴリズムを指定します

説明

key-derivation コマンドは KDF（Key Derivation Function）を設定します。

undo key-derivation コマンドはデフォルトに戻します。

KDF は RSNA メカニズムを使用するネットワークにのみ適用されます。

必須管理フレーム保護が有効な場合、HMAC-SHA256 アルゴリズムを推奨します。

例

HMAC-SHA256 アルゴリズムを指定します。

<AP> system-view

[AP] wlan service-template 1

[AP-wlan-st-1] key-derivation sha256

関連コマンド

- **akm mode**
- **cipher-suite**
- **security-ie**

1.1.10 pmf

🕮 **メモ：**

192bit セキュリティなしの WPA3 エンタープライズは WPA2+管理フレーム保護(**pmf**)と同じです。管理フレーム保護を必須(**Mandatory**)として設定をすることで、192bit セキュリティなしの WPA3 エンタープライズと同等の動作をします。
管理フレーム保護を設定する場合は、KDF の設定”**key-derivation sha1-and-sha256**”をしてください。

Syntax

pmf { **mandatory** | **optional** }

undo pmf

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

mandatory: pmf 必須モードを有効にします。管理フレーム保護をサポートしたクライアントのみ WLAN にアクセスできます。

optional: pmf オプションモード有効にします。すべてのクライアントが WLAN にアクセスできます。

説明

pmf コマンドは管理フレーム保護を有効にします。

undo pmf コマンドはデフォルトに戻します。

管理フレーム保護は、暗号化規格が RSN かつ暗号化方式が CCMP である RSNA メカニズムを使用するネットワークにのみ適用されます。

例

オプションモードで管理フレーム保護を有効にします。

<AP> system-view

[AP] wlan service-template 1

[AP-wlan-st-1] pmf optional

関連コマンド

- **cipher-suite**
- **security-ie**

1.1.11 pmf association-comeback

Syntax

pmf association-comeback *time*

undo pmf association-comeback

デフォルト

1 秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: アソシエーション復帰時間を指定します。設定範囲は 1~20 秒です。

説明

pmf association-comeback コマンドはアソシエーション復帰時間を設定します。

undo pmf association-comeback コマンドはデフォルトに戻します。

AP がクライアントからのアソシエーション要求もしくは再アソシエーション要求を拒否する場合、AP は要求が拒否されたことと、後でクライアントが接続できることを知らせる応答を送ります。この応答にはアソシエーション復帰時間が含まれています。アソシエーション復帰時間が終了すると、AP はクライアントからのアソシエーション要求もしくは再アソシエーション要求の受信を開始します。

例

アソシエーション復帰時間を 2 秒に設定します。

<AP> system-view

[AP] wlan service-template 1

[AP-wlan-st-1] pmf association-comeback 2

1.1.12 pmf saquery retrycount

Syntax

pmf saquery retrycount *count*

undo pmf saquery retrycount

デフォルト

4 回

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

count: SA クエリ要求の最大試行回数を指定します。設定範囲は 1~16 です。

説明

pmf saquery retrycount コマンドは SA クエリ要求を再伝送する試行回数を最大にします。

undo pmf saquery retrycount コマンドはデフォルトに戻します。

最大試行回数に達した後 AP が SA クエリ要求への確認を受信しない場合、AP はクライアントをオフラインにします。

例

SA クエリ要求への最大試行回数を 3 に設定します。

<AP> system-view

[AP] wlan service-template 1

[AP-wlan-st-1] pmf saquery retrycount 3

関連コマンド

- **pmf**
- **pmf saquery retrycount**

1.1.13 pmf saquery retrytimeout

Syntax

pmf saquery retrytimeout *timeout*

undo pmf saquery retrytimeout

デフォルト

200 ミリ秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

timeout: AP が SA クエリ要求を送信する間隔を指定します。設定範囲は 100~500 ミリ秒です。

説明

pmf saquery retrytimeout コマンドは SA クエリ要求を送信する間隔を設定します。

undo pmf saquery retrytimeout コマンドはデフォルトに戻します。

例

SA クエリ要求を送信する間隔を 300 ミリ秒に設定します。

<AP> system-view

[AP] wlan service-template 1

[AP-wlan-st-1] pmf saquery retrytimeout 300

関連コマンド

- **pmf**
- **pmf saquery retrytimeout**

1.1.14 preshared-key

Syntax

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

デフォルト

設定なし

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

pass-phrase: 文字列で PSK を設定します。

raw-key: 16 進数で PSK を設定します。

cipher: 暗号形式で鍵を設定します。

simple: プレーンテキストで鍵を設定します。セキュリティ上の理由から、プレーンテキストで指定された鍵は暗号形式で保存されます。

string: 鍵の文字列を指定します。大文字と小文字を区別します。鍵長は鍵タイプにより変わります。

- **pass-phrase(プレーンテキスト)**－8～63 文字
- **pass-phrase(暗号テキスト)**－8～117 文字
- **raw-key(プレーンテキスト)**－16 進数で 64 桁
- **raw-key(暗号テキスト)**－8～117 文字

説明

preshared-key コマンドは PSK を設定します。

undo preshared-key コマンドは PSK を削除します。

WLAN サービステンプレートが無効で、AKM モードが PSK のときにのみ PSK を設定します。AKM モードが 802.1X のときに PSK を設定した場合、WLAN サービステンプレートは有効ですが PSK コンフィグレーションは反映されません。

WLAN サービステンプレートに設定できる PSK は 1 つだけです。

例

PSK としてプレーンテキストで文字列 12345678 を設定します。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] akm mode psk

[AP-wlan-st-security] akm preshared-key pass-phrase simple 12345678

関連コマンド

akm mode

1.1.15 ptk-lifetime

Syntax

ptk-lifetime *time*

undo ptk-lifetime

デフォルト

43200 秒

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: PTK ライフタイムを指定します。設定範囲は 180~604800 秒です。

説明

ptk-lifetime コマンドは PKT ライフタイムを設定します。

undo ptk-lifetime コマンドはデフォルトに戻します。

サービステンプレートが有効なときに PTK ライフタイムを設定する場合、その設定は既定のタイマが終了した後に適用されます。

例

PTK ライフタイムを 200 秒に設定します。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] ptk-lifetime 200

1.1.16 ptk-rekey enable

Syntax

ptk-rekey enable

undo ptk-rekey enable

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

説明

ptk-rekey enable コマンドは PTK 更新を有効にします。

undo ptk-rekey enable コマンドは PTK 更新を無効にします。

この機能により、設定された PTK の有効期限が切れた後、装置は PTK を更新できます。

例

PTK 更新を有効にします。

<AC> system-view

[AC] wlan service-template security

[AC-wlan-st-security] ptk-rekey enable

関連コマンド

ptk-lifetime

1.1.17 security-ie

Syntax

security-ie { **rsn** | **wpa** }

undo security-ie { **rsn** | **wpa** }

デフォルト

無効

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

rsn: AP に送信されるビーコン/プローブ応答フレームで RSN IE を有効にします。RSN IE は AP の RSN ケーパビリティをアドバタイズします。

wpa: AP に送信されるビーコン/プローブ応答フレームで WPA IE を有効にします。WPA IE は AP の WPA ケーパビリティをアドバタイズします。

説明

security-ie コマンドはビーコンおよびプローブ要求内で RSN IE、あるいは WPA IE を有効にします。

undo security-ie コマンドはビーコンおよびプローブ要求内で OSEN IE、RSN IE、あるいは WPA IE を無効にします。

RSNA ネットワークに暗号化規格を設定する必要があります。WLAN サービステンプレートが無効で、CCMP または TKIP 暗号方式が設定されているときのみ暗号化規格を設定できます。

WPA IE と RSN IE の両方を同じ WLAN サービステンプレートに設定できます。WPA IE と RSN IE は OSEN IE とともに WLAN サービステンプレートに使用できません。

暗号化規格に WPA2 または WPA3 を使用する場合は RSN IE、WPA を使用する場合は WPA IE を設定します。ワイファイアライアンス Anonymous 802.1X AKM の場合、OSEN IE を設定します。

例

ビーコン/プローブ応答で RSN IE を有効にします。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] security-ie rsn

関連コマンド

- **akm mode**
- **cipher-suite**

1.1.18 snmp-agent trap enable wlan usersec

Syntax

snmp-agent trap enable wlan usersec

undo snmp-agent trap enable wlan usersec

デフォルト

WLAN セキュリティの SNMP 通知は、無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan usersec を使用して、WLAN セキュリティの SNMP 通知を有効にします。

WLAN セキュリティの SNMP 通知を無効にするには、**undo snmp-agent trap enable wlan usersec** を使用します。

重要な WLAN セキュリティ イベントを NMS に報告するには、WLAN セキュリティの SNMP 通知を有効にします。

WLAN セキュリティ イベント通知が正しく送信されるようにするには、デバイスで SNMP を設定する必要もあります。

例

WLAN セキュリティの SNMP 通知を有効にします。

<AP> system-view

[AP] snmp-agent trap enable wlan usersec

1.1.19 tkip-cm-time

Syntax

tkip-cm-time *time*

undo tkip-cm-time

デフォルト

0 秒

AP は対策をとりません。

View

WLAN service template view

定義済みユーザロール

network-admin

パラメータ

time: TKIP MIC 失敗ホールド時間を設定します。設定範囲は 0〜3600 秒です。

説明

tkip-cm-time コマンドは TKIP MIC 失敗ホールド時間を設定します。

undo tkip-cm-time コマンドはデフォルトに戻します。

暗号化方式に TKIP が設定されているときにのみ TKIP MIC 失敗ホールド時間を設定します。

サービステンプレートが有効なときに MIC 失敗ホールド時間を設定する場合、その設定は既定のタイマが終了したあとに反映されます。

MIC 失敗ホールド時間内に AP が 2 つの MIC 失敗を検出した場合、AP はすべてのクライアントを 60 秒間分離させます。

例

TKIP MIC 失敗ホールド時間を 180 秒に設定します。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] tkip-cm-time 180

関連コマンド

cipher-suite

1.1.20 wlan password-failure-limit enable

Syntax

wlan password-failure-limit enable [**detection-period** *detection-period*] [**failure-threshold** *failure-threshold*]

undo wlan password-failure-limit enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

detection-period *detection-period*: 検出期間を 5~600 秒の範囲で指定します。デフォルト値は 100 です。

failure-threshold *failure-threshold*: 障害しきい値を 1~100 の範囲で指定します。デフォルト値は 20 です。

説明

wlan password-failure-limit enable コマンドは、パスワード失敗制限を有効します。

undo wlan password-failure-limit enable を使用して パスワード失敗制限を無効にします。

この機能を使用すると、指定された検出期間内にクライアントのパスワードの失敗数が失敗しきい値に達した場合に、ダイナミックブラックリストにクライアントを追加できます。ダイナミックブラックリストの詳細については、コマンドマニュアルのセクション 5 *WLAN アクセスの "WLAN アクセス"*を参照してください。

この機能を設定する場合は、次の制限事項とガイドラインに従ってください。

- この機能は、AKM モードが PSK の場合にのみ有効です。
- この機能は、機能が有効になった後にオンラインになるクライアントに対してのみ有効です。
- STAMGR プロセスが再起動すると、システムはエラー計算を再開します。

例

パスワード失敗制限を有効にし、検出期間を 300 秒に設定し、失敗しきい値を 50 に設定します。

<AP> system-view

[AP] wlan password-failure-limit enable detection-period 300 failure-threshold 50

1.1.21 wpa3

Syntax

v7.5.98 および v7.5.105 の場合：

wpa3 { **enterprise** | **personal** { **mandatory** | **optional** } }

undo wpa3

v7.5.114 以降の場合：

wpa3 { **enterprise** | **enterprise-only-mode** | **enterprise-transition-mode** | **personal** { **mandatory** | **optional** } }

undo wpa3

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

パラメータ

enterprise： WPA3-Enterprise を指定します。

enterprise-only-mode：WPA3-Enterprise モードを必須とすることを指定します。このモードでは、WPA3 をサポートしないクライアントは WLAN にアクセスできません。このモードは v7.5.114 以降のバージョンで実行することができます。

enterprise-transition-mode：WPA3-Enterprise モードへの移行を指定します。このモードでは、WPA3 をサポートしていないクライアントも WLAN にアクセスすることができます。このモードは v7.5.114 以降のバージョンで実行することができます。

personal: WPA3-SAE を指定します。

mandatory: 必須のセキュリティ モードを指定します。このモードでは、WPA3 をサポートしていないクライアントは WLAN にアクセスできません。

optional: オプションのセキュリティ モードを指定します。このモードでは、WPA3 をサポートしていないクライアントが WLAN にアクセスできます。

説明

wpa3 を使用して WPA3 を有効にし、WPA3 セキュリティ モードを設定します。

undo wpa3 を使用して WPA3 を無効にします。

WPA3-Enterprise を使用するには、cipher suite を GCMP に、security IE を RSN に設定します。WPA3-SAE を使用するには、cipher suite を CCMP に、security IE を RSN に設定します。ベスト プラクティスとして、WPA3 セキュリティ モードを指定する場合は、management frame protection(pmf)を有効にします。

注意：

service template を正常に有効にするには、その service template で次の機能を組み合わせて使用しないでください。

- WPA3 security mode.
- FT（Fast BSS Transition）
- Enhanced open system authentication.

FT（Fast BSS Transition）の詳細については、セクション 9 *WLAN ローミング*“*WLAN ローミング*“ を参照してください。

例

WPA3 セキュリティモードをパーソナルレベルの必須モードに設定します。

<AP> system-view

[AP] wlan service-template security

[AP-wlan-st-security] wpa3 personal mandatory

関連コマンド

- **cipher-suite**
- **security-ie**

目次

このセクションのページは **8-x-x** です。

2 章 WIPS 2-1
2.1 WIPS の設定コマンド 2-1
2.1.1 access-scan 2-1
2.1.2 ap-channel-change 2-2
2.1.3 ap-classification rule 2-3
2.1.4 ap-flood 2-4
2.1.5 ap-impersonation 2-5
2.1.6 apply ap-classification rule 2-6
2.1.7 apply classification policy 2-7
2.1.8 apply countermeasure policy 2-8
2.1.9 apply detect policy 2-9
2.1.10 apply signature policy 2-10
2.1.11 apply signature rule 2-11
2.1.12 ap-rate-limit 2-12
2.1.13 ap-spoofing 2-13
2.1.14 ap-timer 2-14
2.1.15 association-table-overflow 2-15
2.1.16 authentication 2-16
2.1.17 block mac-address 2-17
2.1.18 classification policy 2-18
2.1.19 client-association fast-learn enable 2-19
2.1.20 client-online 2-20
2.1.21 client-rate-limit 2-21
2.1.22 client-spoofing 2-22
2.1.23 client-timer 2-23
2.1.24 countermeasure adhoc 2-24
2.1.25 countermeasure attack all 2-25
2.1.26 countermeasure attack deauth-broadcast 2-26
2.1.27 countermeasure attack disassoc-broadcast 2-27
2.1.28 countermeasure attack honeypot-ap 2-28
2.1.29 countermeasure attack hotspot-attack 2-29
2.1.30 countermeasure attack ht-40-mhz-intolerance 2-30
2.1.31 countermeasure attack malformed-packet 2-31
2.1.32 countermeasure attack man-in-the-middle 2-32
2.1.33 countermeasure attack omerta 2-33
2.1.34 countermeasure attack power-save 2-34

2.1.35 countermeasure attack soft-ap 2-35
2.1.36 countermeasure attack unencrypted-trust-client 2-36
2.1.37 countermeasure attack weak-iv 2-37
2.1.38 countermeasure attack windows-bridge 2-38
2.1.39 countermeasure enhance 2-39
2.1.40 countermeasure external-ap 2-40
2.1.41 countermeasure mac-address 2-41
2.1.42 countermeasure misassociation-client 2-42
2.1.43 countermeasure misconfigured-ap 2-43
2.1.44 countermeasure packet-sending-interval 2-44
2.1.45 countermeasure policy 2-45
2.1.46 countermeasure potential-authorized-ap 2-46
2.1.47 countermeasure potential-external-ap 2-47
2.1.48 countermeasure potential-rogue-ap 2-48
2.1.49 countermeasure rogue-ap 2-49
2.1.50 countermeasure unauthorized-client 2-50
2.1.51 countermeasure uncategorized-ap 2-51
2.1.52 countermeasure uncategorized-client 2-52
2.1.53 deauthentication-broadcast 2-53
2.1.54 deauth-spoofing 2-54
2.1.55 detect dissociate-client enable 2-55
2.1.56 detect policy 2-56
2.1.57 detect signature 2-57
2.1.58 disassociation-broadcast 2-58
2.1.59 discovered-ap 2-59
2.1.60 display wips sensor 2-60
2.1.61 display wips statistics 2-61
2.1.62 display wips virtual-security-domain countermeasure record 2-65
2.1.63 display wips virtual-security-domain device 2-67
2.1.64 embedded-oui-classify enable 2-73
2.1.65 export oui 2-74
2.1.66 flood association-request 2-75
2.1.67 flood authentication 2-76
2.1.68 flood beacon 2-77
2.1.69 flood block-ack 2-78
2.1.70 flood cts 2-79
2.1.71 flood deauthentication 2-80
2.1.72 flood disassociation 2-82
2.1.73 flood eap-failure 2-83
2.1.74 flood eapol-logoff 2-84
2.1.75 flood eapol-start 2-85
2.1.76 flood eap-success 2-86
2.1.77 flood null-data 2-87

2.1.78 flood probe-request 2-88
2.1.79 flood reassociation-request 2-89
2.1.80 flood rts 2-90
2.1.81 frame-type 2-91
2.1.82 honeypot-ap 2-92
2.1.83 hotspot-attack 2-93
2.1.84 hotspot ssid 2-94
2.1.85 ht-40mhz-intolerance 2-95
2.1.86 ht-greenfield 2-96
2.1.87 ignorelist 2-97
2.1.88 import hotspot 2-98
2.1.89 import oui 2-99
2.1.90 invalid-oui-classify illegal 2-100
2.1.91 mac-address 2-101
2.1.92 malformed duplicated-ie 2-102
2.1.93 malformed fata-jack 2-103
2.1.94 malformed illegal-ibss-ess 2-104
2.1.95 malformed invalid-address-combination 2-105
2.1.96 malformed invalid-assoc-req 2-106
2.1.97 malformed invalid-auth 2-107
2.1.98 malformed invalid-deauth-code 2-108
2.1.99 malformed invalid-disassoc-code 2-109
2.1.100 malformed invalid-ht-ie 2-110
2.1.101 malformed invalid-ie-length 2-111
2.1.102 malformed invalid-pkt-length 2-112
2.1.103 malformed large-duration 2-113
2.1.104 malformed null-probe-resp 2-114
2.1.105 malformed overflow-eapol-key 2-115
2.1.106 malformed overflow-ssid 2-116
2.1.107 malformed redundant-ie 2-117
2.1.108 man-in-the-middle 2-118
2.1.109 manual-classify mac-address 2-119
2.1.110 match all (AP classification rule view) 2-120
2.1.111 match all (signature view) 2-121
2.1.112 omerta 2-122
2.1.113 oui 2-123
2.1.114 pattern 2-124
2.1.115 permit-channel 2-126
2.1.116 power-save 2-127
2.1.117 prohibited-channel 2-129
2.1.118 random-mac-scan 2-130
2.1.119 report-interval 2-131
2.1.120 reset wips embedded-oui 2-132

2.1.121 reset wips statistics 2-133
2.1.122 reset wips virtual-security-domain 2-134
2.1.123 reset wips virtual-security-domain countermeasure record 2-135
2.1.124 rssi-change-threshold 2-136
2.1.125 rssi-threshold 2-137
2.1.126 rssi 2-138
2.1.127 security 2-139
2.1.128 select sensor all 2-140
2.1.129 seq-number 2-141
2.1.130 signature policy 2-142
2.1.131 signature rule 2-143
2.1.132 soft-ap 2-144
2.1.133 ssid (AP classification rule view) 2-145
2.1.134 ssid (signature view) 2-146
2.1.135 ssid-length 2-147
2.1.136 trust mac-address 2-148
2.1.137 trust oui 2-149
2.1.138 trust ssid 2-150
2.1.139 unencrypted-authorized-ap 2-151
2.1.140 unencrypted-trust-client 2-152
2.1.141 up-duration 2-153
2.1.142 virtual-security-domain 2-154
2.1.143 weak-iv 2-155
2.1.144 windows-bridge 2-156
2.1.145 wips(system view) 2-157
2.1.146 wips(radio view) 2-158
2.1.147 wips virtual-security-domain 2-159
2.1.148 wireless-bridge 2-160

2章 WIPS

🕮 **メモ：**

- WIPS の機能はソフトウェアバージョン 7.5.105 を含む以降のソフトウェアからサポートしています。

2.1 WIPSの設定コマンド

2.1.1 access-scan

Syntax

access-scan enable

undo access-scan enable

デフォルト

無効

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がチャネル変更のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にチャネル変更を検出してもアラームを引き起こしません。

説明

ap-channel-change コマンドはアクセスサービスを提供しながら、AP による WIPS スキャンの実行を無効します。

このコマンドは、WIPS の検出および保護機能を強化しますが、アクセスサービス機能を低下させます

例

アクセスサービスを提供しながら、WIPS スキャンを実行するように AP を設定します。

<AP> system-view

[AP] wips

[AP] access-scan enable

2.1.2 ap-channel-change

Syntax

ap-channel-change [**quiet** *quiet-value*]

undo ap-channel-change

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がチャネル変更のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にチャネル変更を検出してもアラームを引き起こしません。

説明

ap-channel-change コマンドはチャネル変更を設定します。

undo ap-channel-change コマンドはチャネル変更の検出を無効にします。

例

チャネル変更の検出を有効にし、遅延時間を 5 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-channel-change quiet 5

2.1.3 ap-classification rule

Syntax

ap-classification rule *rule-id*

undo ap-classification rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で AP 分類ルールを指定します。値の範囲は 1～65535 です。

説明

ap-classification rule コマンドは AP 分類ルールを作成し、その view に移行します。AP 分類ルールがすでに存在する場合、**ap-classification rule** コマンドで AP 分類ルール view に移行します。

undo ap-classification rule コマンドは AP 分類ルールを削除します。

例

AP classification rule 1 を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

2.1.4 ap-flood

Syntax

ap-flood [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *

undo ap-flood

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

apnum *apnum-value*: AP 数しきい値を指定します。値の範囲は 10～200 です。デフォルト値は 80 です。

exceed *exceed-value*: 超過を許可された AP の最大数を指定します。*exceed-value* 引数の値の範囲は 10～200 です。デフォルト値は 80 です。AP の数が、AP 数しきい値と、超過を許可された AP の最大数の合計を超える場合、WIPS は AP フラッド攻撃アラームを引き起こします。

quiet *quiet-value*: WIPS が AP フラッド攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP フラッド攻撃を検出してもアラームを引き起こしません。

説明

ap-flood コマンドは AP フラッド攻撃検出を設定します。

undo ap-flood コマンドは AP フラッド攻撃検出を無効にします。

例

AP フラッド攻撃検出を有効にし、*apnum-value*、*exceed-value*、*quiet-value* をそれぞれ 50、50、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-flood apnum 50 exceed 50 quiet 100

2.1.5 ap-impersonation

Syntax

ap-impersonation [**quiet** *quiet-value*]

undo ap-impersonation

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP なりすまし攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト時間は 600 秒です。WIPS は遅延時間内に AP なりすまし攻撃を検出してもアラームを引き起こしません。

説明

ap-impersonation コマンドは AP なりすまし攻撃検出を設定します。

undo ap-impersonation コマンドはデフォルトに戻します。

例

AP なりすまし攻撃検出を有効にし、遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-impersonation quiet 360

2.1.6 apply ap-classification rule

Syntax

apply ap-classification rule *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }

undo apply ap-classification rule *rule-id*

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で AP 分類ルールを指定します。ID の値の範囲は 1～65535 です。

authorized-ap: 許可された AP として AP 分類ルールに一致する AP を指定します。

external-ap: 外部 AP

misconfigured-ap: 不良コンフィグレーション AP として AP 分類ルールに一致する AP を指定します。

rogue-ap: 不正な AP として AP 分類ルールに一致する AP を指定します。

level: AP 分類ルールに一致する AP に対して重大度レベルを指定します。レベルの範囲は 1～100 です。デフォルトレベルは 50 です。

説明

apply ap-classification rule コマンドは分類ポリシーに AP 分類ルールを設定します。

undo apply ap-classification rule コマンドはデフォルトに戻します。

例

分類ポリシー**home** に AP classification rule 1 を設定します。不正な AP として AP classification rule 1 に一致する AP を指定します。重大度レベルを 80 に設定します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] apply ap-classification rule 1 rogue-ap severity-level 80

関連コマンド

ap-classification rule

2.1.7 apply classification policy

Syntax

apply classification policy *policy-name*

undo apply classification policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply classification policy コマンドは分類ポリシーを VSD（Virtual Security Domain）に適用します。

undo apply classification policy コマンドは VSD から分類ポリシーを削除します。

例

分類ポリシー**policy1** を VSD **home** に適用します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain home

[AP-wips-vsd-home] apply classification policy policy1

2.1.8 apply countermeasure policy

Syntax

apply countermeasure policy *policy-name*

undo apply countermeasure policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply countermeasure policy コマンドは対策ポリシーを VSD に適用します。

undo apply countermeasure policy コマンドは VSD から対策ポリシーを削除します。

例

対策ポリシー**policy2** を VSD **home** に適用します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain home

[AP-wips-vsd-home] apply countermeasure policy policy2

2.1.9 apply detect policy

Syntax

apply detect policy *policy-name*

undo apply detect policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply detect policy コマンドは攻撃検出ポリシーを VSD に適用します。

undo apply detect policy コマンドは VSD から攻撃検出ポリシーを削除します。

例

攻撃検出ポリシー**policy2** を VSD **home** に適用します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain home

[AP-wips-vsd-home] apply detect policy policy2

2.1.10 apply signature policy

Syntax

apply signature policy *policy-name*

undo apply signature policy *policy-name*

デフォルト

設定なし

View

VSD view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

apply signature policy コマンドは署名ポリシーを VSD に適用します。

undo apply signature policy コマンドはデフォルトに戻します。

例

署名ポリシー**policy1** を VSD **home** に適用します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain home

[AP-wips-vsd-home] apply signature policy policy1

2.1.11 apply signature rule

Syntax

apply signature rule *rule-id*

undo apply signature rule *rule-id*

デフォルト

設定なし

View

Signature policy view

定義済みユーザロール

network-admin

パラメータ

rule-id: ID で署名を指定します。値の範囲は 1～65535 文字です。

説明

apply signature rule コマンドは署名ポリシーに署名を設定します。

undo apply signature rule コマンドはデフォルトに戻します。

例

signature 1 を署名ポリシー**office** に設定します。

<AP> system-view

[AP] wips

[AP-wips] signature policy office

[AP-wips-sig-office] apply signature rule 1

2.1.12 ap-rate-limit

Syntax

ap-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo ap-rate-limit

デフォルト

学習した AP エントリのための統計値収集間隔： 60 秒

遅延時間： 1200 秒

AP エントリしきい値： 64

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 学習した AP エントリのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS が AP エントリ攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold *threshold-value*: AP エントリ攻撃アラームを引き起こす AP エントリ数を指定します。*threshold-value* 引数の値の範囲は 1～4096 です。

説明

ap-rate-limit コマンドは AP エントリの学習を制限します。

undo ap-rate-limit コマンドはデフォルトに戻します。

例

AP エントリの学習を制限します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-rate-limit interval 60 quiet 1600 threshold 100

2.1.13 ap-spoofing

Syntax

ap-spoofing [**quiet** *quiet-value*]

undo ap-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が AP スプーフィング攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内に AP エントリ攻撃を検出してもアラームを引き起こしません。

説明

ap-spoofing コマンドは AP スプーフィング攻撃を有効にします。

undo ap-spoofing コマンドは AP スプーフィング攻撃を無効にします。

例

AP スプーフィング検出を有効にし、遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-spoofing quiet 360

2.1.14 ap-timer

Syntax

ap-timer [**inactive** *inactive-value* **aging** *aging-value*]

undo ap-timer

デフォルト

非アクティブ時間： 300 秒

エージングタイマ： 600 秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

inactive *inactive-value*: 非アクティブ時間を指定します。*inactive-value* 引数の値の範囲は 60～1200 秒です。指定された非アクティブ時間内に AP がフレームを送受信しない場合、WIPS は AP を非アクティブ状態に設定します。

aging *aging-value*: エージングタイマを指定します。値の範囲は 120～86400 秒です。指定されたエージングタイマ内に AP がフレームを送受信しない場合、WIPS はエントリを削除します。エージングタイマは非アクティブ時間より大きくなければなりません。

説明

ap-timer コマンドは AP エントリタイマを設定します。

undo ap-timer コマンドはデフォルトに戻します。

例

非アクティブ時間を 120 秒、エージングタイマを 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ap-timer inactive 120 aging 360

2.1.15 association-table-overflow

Syntax

association-table-overflow [**quiet** *quiet-value*]

undo association-table-overflow

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がアソシエーション/再アソシエーション DoS 攻撃アラームを引き起こした後、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にアソシエーション/再アソシエーション DoS 攻撃を検出してもアラームを引き起こしません。

説明

association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を設定します。

undo association-table-overflow コマンドはアソシエーション/再アソシエーション DoS 攻撃検出を無効にします。

例

アソシエーション/再アソシエーション DoS 攻撃検出を有効にし、遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] association-table-overflow quiet 100

2.1.16 authentication

Syntax

authentication { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }

undo authentication

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

equal: 指定された認証モードと等しい認証モードを整合します。

include: 指定された認証モードを含む認証モードを整合します。

802.1x: 802.1X 認証モードを指定します。

none: 認証モードは指定されません。

other: 802.1X と PSK 以外の認証モードを指定します。

psk: PSK 認証モードを指定します。

説明

authentication コマンドは AP の認証モードを整合するために AP 分類ルールを設定します。

undo authentication コマンドはデフォルトに戻します。

例

PSK 認証モードを使用する AP を整合するために AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] authentication equal psk

2.1.17 block mac-address

Syntax

block mac-address *mac-address*

undo block mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の無線 MAC アドレス(BSSID)もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

all: すべての MAC アドレスを指定します。

説明

block mac-address コマンドはスタティック禁止装置リストに MAC アドレスを追加します。

undo block mac-address コマンドはスタティック禁止装置リストから 1 つもしくはすべての MAC アドレスを削除します。

例

スタティック禁止装置リストに MAC アドレス **78AC-C0AF-944F** を追加します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] block mac-address 78AC-C0AF-944F

2.1.18 classification policy

Syntax

classification policy *policy-name*

undo classification policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 分類ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

classification policy コマンドは分類ポリシーを作成し、その view に移行します。

undo classification policy コマンドは分類ポリシーを削除します。

例

分類ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home]

2.1.19 client-association fast-learn enable

Syntax

client-association fast-learn enable

undo client-association fast-learn enable

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

説明

client-online コマンドはクライアントアソシエーションエントリの高速学習を有効します。

クライアントアソシエーションエントリは、クライアントが AP にアソシエートした後に AC に保存されるエントリです。

このコマンドが設定されていない場合、センサがクライアントアソシエーションエントリを学習できるのは、クライアントが AP に正常にアソシエートされた後だけです。このコマンドが設定されると、センサはアソシエーションプロセス中にクライアントアソシエーションエントリを学習できます。

センサがアソシエーションプロセス中にクライアントアソシエーションエントリを学習した場合、センサは AP とクライアント間のアソシエーション要求または応答を検出するたびにエントリを更新します。

このコマンドにより、アソシエーションの効率は向上しますが、アソシエーションの精度は低下します。ベストプラクティスとして、ネットワークで高速な攻撃の検出と対策が必要な場合にのみ、このコマンドを設定します。

例

クライアントアソシエーションエントリの高速学習を有効にします。

<AP> system-view

[AP] wips

[AP-wips] detect policy

2.1.20 client-online

Syntax

client-online *value1* [**to** *value2*]

undo client-online

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 **to** *value2*: AP に紐付けられたクライアント数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～128 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

client-online コマンドは AP に紐付いたクライアント数を整合するために AP 分類ルールを設定します。

undo client-online コマンドはデフォルトに戻します。

例

20～40 のクライアントに紐付いた AP を整合するために、AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] client-online 20 to 40

2.1.21 client-rate-limit

Syntax

client-rate-limit [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo client-rate-limit

デフォルト

学習したクライアントエントリのための統計値収集間隔： 60 秒

遅延時間： 1200 秒

クライアントエントリしきい値： 512

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 学習したクライアントエントリのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。

quiet *quiet-value*: WIPS がクライアントエントリ攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 1200～3600 秒です。WIPS は遅延時間内にクライアントエントリ攻撃を検出してもアラームを引き起こさず、AP エントリ学習を停止します。

threshold *threshold-value*: クライアントエントリ攻撃アラームを引き起こすクライアントエントリ数を指定します。*threshold-value* 引数の値の範囲は 1～4096 です。

説明

client-rate-limit コマンドはクライアントエントリの学習を制限します。

undo client-rate-limit コマンドはデフォルトに戻します。

例

クライアントエントリの学習を制限します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] client-rate-limit interval 80 quiet 1600 threshold 100

2.1.22 client-spoofing

Syntax

client-spoofing [**quiet** *quiet-value*]

undo client-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がクライアントスプーフィング攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトの遅延時間は 600 秒です。WIPS は遅延時間内にクライアントスプーフィング攻撃を検出してもアラームを引き起こしません。

説明

client-spoofing コマンドはクライアントスプーフィング攻撃検出を有効にします。

undo client-spoofing コマンドはクライアントスプーフィング攻撃検出を無効にします。

例

クライアントスプーフィング攻撃検出を有効にし、遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] client-spoofing quiet 360

2.1.23 client-timer

Syntax

client-timer inactive *inactive-value* **aging** *aging-value*

undo client-timer

デフォルト

非アクティブ時間： 300 秒

エージングタイマ： 600 秒

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

inactive *inactive-value*: 非アクティブ時間を指定します。*inactive-value* 引数の値の範囲は 60～1200 秒です。指定された非アクティブ時間内にクライアントがフレームを送受信しない場合、WIPS はクライアントを非アクティブ状態に設定します。

aging *aging-value*: エージングタイマを指定します。値の範囲は 120～86400 秒です。指定されたエージングタイマ内にクライアントがフレームを送受信しない場合、WIPS はエントリを削除します。エージングタイマは非アクティブ時間より大きくなければなりません。

説明

client-timer コマンドはクライアントエントリタイマを設定します。

undo client-timer コマンドはデフォルトに戻します。

例

非アクティブ時間を 120 秒、エージングタイマを 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] client-timer inactive 120 aging 360

2.1.24 countermeasure adhoc

Syntax

countermeasure adhoc

undo countermeasure adhoc

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure adhoc コマンドはアドホックデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure adhoc コマンドはデフォルトに戻します。

例

アドホックデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure adhoc

2.1.25 countermeasure attack all

Syntax

countermeasure attack all

undo countermeasure attack all

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack all コマンドはすべての攻撃者に対策を講じるために WIPS を有効にします。

undo countermeasure attack all コマンドはデフォルトに戻します。

例

すべての攻撃者に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack all

2.1.26 countermeasure attack deauth-broadcast

Syntax

countermeasure attack deauth-broadcast

undo countermeasure attack deauth-broadcast

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure deauth-broadcast コマンドはブロードキャスト認証解除攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure deauth-broadcast コマンドはデフォルトに戻します。

例

ブロードキャスト認証解除攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack deauth-broadcast

2.1.27 countermeasure attack disassoc-broadcast

Syntax

countermeasure attack disassoc-broadcast

undo countermeasure attack disassoc-broadcast

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack disassoc-broadcast コマンドはブロードキャストディスアソシエーション攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack disassoc-broadcast コマンドはデフォルトに戻します。

例

ブロードキャストディスアソシエーション攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack disassoc-broadcast

2.1.28 countermeasure attack honeypot-ap

Syntax

countermeasure attack honeypot-ap

undo countermeasure attack honeypot-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack honeypot-ap コマンドはハニーポット AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack honeypot-ap コマンドはデフォルトに戻します。

例

ハニーポット AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack honeypot-ap

2.1.29 countermeasure attack hotspot-attack

Syntax

countermeasure attack hotspot-attack

undo countermeasure attack hotspot-attack

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack hotspot-attack コマンドはホットスポット攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack hotspot-attack コマンドはデフォルトに戻します。

例

ホットスポット攻撃を開始するデバイスに対策を講じるためにWIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack hotspot-attack

2.1.30 countermeasure attack ht-40-mhz-intolerance

Syntax

countermeasure attack ht-40-mhz-intolerance

undo countermeasure attack ht-40-mhz-intolerance

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack ht-40-mhz-intolerance コマンドは 40MHz 帯域幅モードが無効のデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack ht-40-mhz-intolerance コマンドはデフォルトに戻します。

例

40MHz 帯域幅モードが無効のデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack ht-40-mhz-intolerance

2.1.31 countermeasure attack malformed-packet

Syntax

countermeasure attack malformed-packet

undo countermeasure attack malformed-packet

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack malformed-packet コマンドは不正な形式のパケットを送信するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack malformed-packet コマンドはデフォルトに戻します。

例

不正な形式のパケットを送信するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack malformed-packet

2.1.32 countermeasure attack man-in-the-middle

Syntax

countermeasure attack man-in-the-middle

undo countermeasure attack man-in-the-middle

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack man-in-the-middle コマンドは MITM 攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack man-in-the-middle コマンドはデフォルトに戻します。

例

MITM 攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack man-in-the-middle

2.1.33 countermeasure attack omerta

Syntax

countermeasure attack omerta

undo countermeasure attack omerta

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack omerta コマンドは Omerta 攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack omerta コマンドはデフォルトに戻します。

例

Omerta 攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack omerta

2.1.34 countermeasure attack power-save

Syntax

countermeasure attack power-save

undo countermeasure attack power-save

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack power-save コマンドは節電攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack power-save コマンドはデフォルトに戻します。

例

節電攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack power-save

2.1.35 countermeasure attack soft-ap

Syntax

countermeasure attack soft-ap

undo countermeasure attack soft-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack soft-ap コマンドはソフト AP に対策を講じるために WIPS を有効にします。

undo countermeasure attack soft-ap コマンドはデフォルトに戻します。

例

ソフト AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack soft-ap

2.1.36 countermeasure attack unencrypted-trust-client

Syntax

countermeasure attack unencrypted-trust-client

undo countermeasure attack unencrypted-trust-client

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack unencrypted-trust-client コマンドは暗号化されていない許可されたクライアントに対策を講じるために WIPS を有効にします。

undo countermeasure attack unencrypted-trust-client コマンドはデフォルトに戻します。

例

暗号化されていない許可されたクライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack unencrypted-trust-client

2.1.37 countermeasure attack weak-iv

Syntax

countermeasure attack weak-iv

undo countermeasure attack weak-iv

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack weak-iv コマンドは Weak IV を使用するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack weak-iv コマンドはデフォルトに戻します。

例

Weak IV を使用するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack weak-iv

2.1.38 countermeasure attack windows-bridge

Syntax

countermeasure attack windows-bridge

undo countermeasure attack windows-bridge

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure attack windows-bridge コマンドは Windows ブリッジ攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

undo countermeasure attack windows-bridge コマンドはデフォルトに戻します。

例

Windows ブリッジ攻撃を開始するデバイスに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure attack windows-bridge

2.1.39 countermeasure enhance

Syntax

countermeasure enhance

undo countermeasure enhance

デフォルト

エンハンスされた対策モードは、無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

エンハンスされた対策モードを有効にするには、**countermeasure enhance** します。

undo countermeasure enhance を使用してデフォルトに戻します。

このコマンドを設定して、デュアルバンド クライアントが不正 AP 上の同じ SSID を共有する 2 つの無線間でローミングできないようにします。

例

エンハンスされた対策モードを有効にします。

```
<AP> system-view
[AP] wips
[AP-wips] countermeasure policy home
[AP-wips-cms-home] countermeasure enhance
```

2.1.40 countermeasure external-ap

Syntax

countermeasure external-ap

undo countermeasure external-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure external-ap コマンドは外部の AP に対策を講じるために WIPS を有効にします。

undo countermeasure external-ap コマンドはデフォルトに戻します。

例

#外部の AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure external-ap

2.1.41 countermeasure mac-address

Syntax

countermeasure mac-address *mac-address*

undo countermeasure mac-address { *mac-address* | **all** }

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の無線 MAC アドレス(BSSID)もしくはクライアントの MAC アドレスを H-H-H 形式で指定します。

all: すべての AP とクライアントを指定します。

説明

countermeasure mac-address コマンドは指定された MAC アドレスを持つ装置に対策を講じるために WIPS を有効にします。

undo countermeasure mac-address コマンドは設定を削除します。

countermeasure mac-address コマンドを複数回設定することで、複数の装置に対策を講じるように WIPS を有効化できます。

例

MAC アドレス **2a11-1fa1-141f** を持つ装置に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure mac-address 2a11-1fa1-141f

2.1.42 countermeasure misassociation-client

Syntax

countermeasure misassociation-client

undo countermeasure misassociation-client

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure misassociation-client コマンドは間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

undo countermeasure misassociation-client コマンドはデフォルトに戻します。

例

間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure misassociation-client

2.1.43 countermeasure misconfigured-ap

Syntax

countermeasure misconfigured-ap

undo countermeasure misconfigured-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure misconfigured-ap コマンドは間違って設定された AP に対策を講じるために WIPS を有効にします。

undo countermeasure misconfigured-ap コマンドはデフォルトに戻します。

例

間違って紐付いたクライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure misconfigured-ap

2.1.44 countermeasure packet-sending-interval

Syntax

countermeasure packet-sending-interval *interval*

undo countermeasure packet-sending-interval

デフォルト

30 ミリ秒

View

Countermeasure policy view

定義済みユーザロール

network-admin

パラメータ

interval: センサが対策パケットを送信する間隔を指定します。値の範囲は 1~100 ミリ秒です。

説明

countermeasure policy コマンドは、センサが対策パケットを送信する間隔を指定します。

undo countermeasure policy コマンドは、対策ポリシーを削除します。

チャネル内に不正デバイスが検出された場合に、センサがチャネル内で対策パケットを送信できるようにするには、このコマンドを設定します。センサはスキャン期間内にのみチャネル内で対策パケットを送信し、センサが対策パケットを送信する間隔を指定できます。チャネルスキャンの詳細については、コマンドマニュアルのセクション 8 の *Radio リソース管理 "Radio リソース管理"* を参照してください。

例

10 ミリ秒ごとに対策パケットを送信するようにセンサを設定します。

<AP> system-view

[AP] wips

[AP] countermeasure policy home

[AP-wips-cms-home] countermeasure packet-sending-interval 10

2.1.45 countermeasure policy

Syntax

countermeasure policy *policy-name*

undo countermeasure policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 対策ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

countermeasure policy コマンドは対策ポリシーを作成し、その view に移行します。

undo countermeasure policy コマンドは対策ポリシーを削除します。

例

対策ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home]

2.1.46 countermeasure potential-authorized-ap

Syntax

countermeasure potential-authorized-ap

undo countermeasure potential-authorized-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-authorized-ap コマンドは潜在的に認可された AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-authorized-ap コマンドはデフォルトに戻します。

例

潜在的に認可された AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure potential-authorized-ap

2.1.47 countermeasure potential-external-ap

Syntax

countermeasure potential-external-ap

undo countermeasure potential-external-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-external-ap コマンドは潜在的外部 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-external-ap コマンドはデフォルトに戻します。

例

対策ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure potential-external-ap

2.1.48 countermeasure potential-rogue-ap

Syntax

countermeasure potential-rogue-ap

undo countermeasure potential-rogue-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure potential-rogue-ap コマンドは潜在的な不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure potential-rogue-ap コマンドはデフォルトに戻します。

例

潜在的な不正 AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure potential-rogue-ap

2.1.49 countermeasure rogue-ap

Syntax

countermeasure rogue-ap

undo countermeasure rogue-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure rogue-ap コマンドは不正 AP に対策を講じるために WIPS を有効にします。

undo countermeasure rogue-ap コマンドはデフォルトに戻します。

例

不正な AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure rogue-ap

2.1.50 countermeasure unauthorized-client

Syntax

countermeasure unauthorized-client

undo countermeasure unauthorized-client

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure unauthorized-client コマンドは未許可クライアントに対策を講じるために WIPS を有効にします。

undo countermeasure unauthorized-client コマンドはデフォルトに戻します。

例

未許可クライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure unauthorized-client

2.1.51 countermeasure uncategorized-ap

Syntax

countermeasure uncategorized-ap

undo countermeasure uncategorized-ap

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure uncategorized-ap コマンドは未分類の AP に対策を講じるために WIPS を有効にします。

undo countermeasure uncategorized-ap コマンドはデフォルトに戻します。

例

未分類の AP に対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure uncategorized-ap

2.1.52 countermeasure uncategorized-client

Syntax

countermeasure uncategorized-client

undo countermeasure uncategorized-client

デフォルト

無効

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

countermeasure uncategorized-client コマンドは未分類のクライアントに対策を講じるために WIPS を有効にします。

undo countermeasure uncategorized-client コマンドはデフォルトに戻します。

例

未分類のクライアントに対策を講じるために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-cms-home] countermeasure uncategorized-client

2.1.53 deauthentication-broadcast

Syntax

deauthentication-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo deauthentication-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証取り消し攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。WIPS は遅延時間内にブロードキャスト認証取り消し攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証取り消し攻撃アラームを引き起こすブロードキャスト認証取り消しの数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

deauthentication-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を設定します。

undo deauthentication-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を無効にします。

例

ブロードキャスト認証取り消し攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] deauthentication-broadcast interval 100 threshold 100 quiet 360

2.1.54 deauth-spoofing

Syntax

deauth-spoofing [**quiet** *quiet*]

undo deauth-spoofing

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet*: スプーフィング認証解除フレームで WIPS がアラームをトリガーした後の待機時間を指定します。*quiet-value* 引数の値の範囲は 5~604800 秒で、デフォルトの待機時間は 600 秒です。WIPS は、待機時間内にスプーフィング認証解除フレームを検出してもアラームをトリガーしません。

説明

deauth-spoofing コマンドはスプーフィング認証解除フレーム検出を設定します。

undo deauth-spoofing コマンドはスプーフィング認証解除フレーム検出を無効にします。

例

スプーフィング認証解除フレーム検出を有効にし、クワイエットタイムを 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] deauth-spoofing quiet 100

2.1.55 detect dissociate-client enable

Syntax

detect dissociate-client enable

undo detect dissociate-client enable

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

説明

detect policy コマンドは WIPS が関連付けられていないクライアントを検出できるようにします。

undo detect policy コマンドは WIPS が関連付けられていないクライアントを検出できないようにします。

例

関連付けられていないクライアントを検出するために WIPS を有効にします。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] detect dissociate-client enable

2.1.56 detect policy

Syntax

detect policy *policy-name*

undo detect policy *policy-name*

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

policy-name: 攻撃検出ポリシー名を指定します。大文字と小文字を区別します。設定範囲は 1～63 文字です。

説明

detect policy コマンドは攻撃検出ポリシーを作成し、その view に移行します。

undo detect policy コマンドは攻撃検出ポリシーを削除します。

例

攻撃検出ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home]

2.1.57 detect signature

Syntax

detect signature [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo detect

デフォルト

有効

View

Signature policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 署名に一致するパケットのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が user-defined 攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内に user-defined 攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: user-defined 攻撃アラームを引き起こす、署名に一致したパケット数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

detect signature コマンドは署名に基づく user-define 攻撃検出を有効にします。

undo detect signature コマンドは署名に基づく user-define 攻撃検出を無効にします。

例

署名に基づく user-define 攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、60、100、360 に設定します。

<AP> system-view

[AP] wips

[AP-wips] signature policy home

[AP-wips-sig-home] detect signature interval 60 threshold 100 quiet 360

2.1.58 disassociation-broadcast

Syntax

disassociation-broadcast [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo disassociation-broadcast

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロードキャスト認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの統計値収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロードキャスト認証取り消し攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルト値は 600 秒です。WIPS は遅延時間内にブロードキャスト認証取り消し攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロードキャスト認証取り消し攻撃アラームを引き起こす、ブロードキャスト認証取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

disassociation-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を有効にします。

undo disassociation-broadcast コマンドはブロードキャスト認証取り消し攻撃検出を無効にします。

例

ブロードキャスト認証取り消し攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] disassociation-broadcast interval 100 threshold 100 quiet 360

2.1.59 discovered-ap

Syntax

discovered-ap *value1* [**to** *value2*]

undo discovered-ap

デフォルト

一致なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 **to** *value2*: AP を検出するセンサの数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 1～128 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

discovered-ap コマンドは AP を検出するセンサの数を整合するために AP 分類ルールを設定します。

undo discovered-ap コマンドはデフォルトに戻します。

例

10～128 のセンサに検出された AP を整合するために、AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] discovered-ap 10 to 128

2.1.60 display wips sensor

Syntax

display wips sensor

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wips sensor コマンドはすべてのセンサに関する情報を表示します。

例

すべてのセンサに関する情報を表示します。

<AP> display wips sensor

```
Total number of sensors: 1
Sensor ID    Sensor name             VSD name            Radio ID   Status
3            fatap                   aaa                 1          Active
```

表 2-1 コマンド出力

フィールド	説明
VSD name	APが属するVSDの名前
Radio ID	WIPSで有効化された無線の名前
Status	センサの状態 ● **Active**ーセンサはWIPSで有効にされます。 ● **Inactive**ーセンサはWIPSで有効にされません。

2.1.61 display wips statistics

Syntax

display wips statistics [**receive** | **virtual-security-domain** *vsd-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

receive: すべての VSD のセンサから AC が受信する攻撃検出統計値情報を表示します。

virtual-security-domain *vsd-name*: 指定された VSD のセンサから AC が受信する攻撃検出統計値情報を表示します。

説明

display wips statistics コマンドはセンサから収集した攻撃検出情報を表示します。

例

すべての VSD のセンサから収集した攻撃検出統計値情報を表示します。

<AP> display wips statistics receive

```
Information from sensor 1
 Information about attack statistics:
   Detected association-request flood messages: 0
   Detected authentication flood messages: 0
   Detected beacon flood messages: 0
   Detected block-ack flood messages: 0
   Detected cts flood messages: 0
   Detected deauthentication flood messages: 0
   Detected disassociation flood messages: 0
   Detected eapol-start flood messages: 0
   Detected null-data flood messages: 0
   Detected probe-request flood messages: 0
   Detected reassociation-request flood messages: 0
   Detected rts flood messages: 0
   Detected eapol-logoff flood messages: 0
   Detected eap-failure flood messages: 0
   Detected eap-success flood messages: 0
   Detected duplicated-ie messages: 0
   Detected fata-jack messages: 0
```

```
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected signature rule messages: 0
Detected 40MHZ messages: 0
Detected power save messages: 0
Detected omerta messages: 0
Detected windows bridge messages: 0
Detected soft AP messages: 0
Detected broadcast disassociation messages: 0
Detected broadcast deauthentication messages: 0
Detected AP impersonate messages: 0
Detected illegal channel 9 messages: 1
```

表 2-2 コマンド出力

フィールド	説明
Information from sensor n	センサ**n** から収集した情報。**n** はセンサのIDをあらわします。
Detected association-request flood messages	紐付け要求フラッドアタック攻撃に対して検出したメッセージの数。
Detected authentication flood messages	認証要求フラッド攻撃に対して検出したメッセージの数。
Detected beacon flood messages	ビーコンフラッド攻撃に対して検出したメッセージの数。

フィールド	説明
Detected block-ack flood messages	ブロックアクトフラッド攻撃に対して検出したメッセージの数。
Detected cts flood messages	CTSフラッド攻撃に対して検出したメッセージの数。
Detected deauthentication flood messages	認証取り消しフラッド攻撃に対して検出したメッセージの数。
Detected disassociation flood messages	紐付け取り消しフラッド攻撃に対して検出したメッセージの数。
Detected eapol-start flood messages	EAPOLスタートフラッド攻撃に対して検出したメッセージの数。
Detected null-data flood messages	ヌルデータフラッド攻撃に対して検出したメッセージの数。
Detected probe-request flood messages	プローブ要求フラッド攻撃に対して検出したメッセージの数。
Detected reassociation-request flood messages	再紐付け要求フラッド攻撃に対して検出したメッセージの数。
Detected rts flood messages	RTSフラッド攻撃に対して検出したメッセージの数。
Detected eapol-logoff flood messages	EAPOLログオフフラッド攻撃に対して検出したメッセージの数。
Detected eap-failure flood messages	EAPOL失敗フラッド攻撃に対して検出したメッセージの数。
Detected eap-success flood messages	EAPOL成功フラッド攻撃に対して検出したメッセージの数。
Detected duplicated-ie messages	複製されたIEをもつ異常パケットに対して検出したメッセージの数。
Detected fata-jack messages	FATAジャック異常パケットに対して検出したメッセージの数。
Detected illegal-ibss-ess messages	異常なIBSSとESS設定をもつ異常パケットに対して検出したメッセージの数。
Detected invalid-address-combination messages	無効な送信元アドレスをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-assoc-req messages	異常な紐付け要求に対して検出したメッセージの数。
Detected invalid-auth messages	異常な認証要求に対して検出したメッセージの数。
Detected invalid-deauth-code messages	無効な認証取り消しコードをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-disassoc-code messages	無効な紐付け取り消しコードをもつ異常パケットに対して検出したメッセージの数。

フィールド	説明
Detected invalid-ht-ie messages	異常なHT IEをもつ異常パケットに対して検出したメッセージの数。
Detected invalid-ie-length messages	無効なIE長をもつ異常パケットに対して検出したメッセージの数。
Detected invalid-pkt-length messages	無効なパケット長をもつ異常パケットに対して検出したメッセージの数。
Detected large-duration messages	オーバーサイズの期間をもつ異常パケットに対して検出したメッセージの数。
Detected null-probe-resp messages	異常なプローブ要求フレームに対して検出したメッセージの数。
Detected overflow-eapol-key messages	オーバーサイズのEAPOL鍵をもつ異常パケットに対して検出したメッセージの数。
Detected overflow-ssid messages	オーバーサイズなSSIDをもつ異常パケットに対して検出したメッセージの数。
Detected redundant-ie messages	冗長なIEをもつ異常パケットに対して検出したメッセージの数。
Detected AP spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs AP)
Detected AP spoof client messages	クライアントスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs client)
Detected AP spoof ad-hoc messages	アドホックスプーフィング攻撃に対して検出したメッセージの数。(AP spoofs Ad hoc)
Detected ad-hoc spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(Ad hoc spoofs AP)
Detected client spoof AP messages	APスプーフィング攻撃に対して検出したメッセージの数。(client spoofs AP)
Detected weak IV messages	ウィークIVに対して検出したメッセージの数。
Detected excess AP messages	APエントリ攻撃に対して検出したメッセージの数。
Detected excess client messages	クライアントエントリ攻撃に対して検出したメッセージの数。
Detected 40MHZ messages	40Hz帯モードで無効化されるクライアントに対して検出したメッセージの数。
Detected power save messages	電力節約攻撃に対して検出したメッセージの数。
Detected omerta messages	Omerta攻撃に対して検出したメッセージの数。
Detected windows bridge messages	Windowsブリッジに対して検出したメッセージの数。
Detected soft AP messages	ソフトAPに対して検出したメッセージの数。

フィールド	説明
Detected broadcast disassociation messages	ブロードキャスト紐付け取り消し攻撃に対して検出したメッセージの数。
Detected broadcast deauthentication messages	ブロードキャスト認証取り消し攻撃に対して検出したメッセージの数。
Detected AP impersonate messages	APなりすまし攻撃に対して検出したメッセージの数。
Detected illegal channel n messages:	禁止されたチャネルに対して検出したメッセージの数。*n*はチャネル番号を示します。

関連コマンド

reset wips statistics

2.1.62 display wips virtual-security-domain countermeasure record

Syntax

display wips virtual-security-domain *vsd-name* **countermeasure record**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

display wips virtual-security-domain countermeasure record コマンドは不正なデバイスに対して WIPS が実行した対策に関する情報が表示されます。

例

WIPS が VSD **office** の不正デバイスに対して行った対策に関する情報を表示します。

<AP> display wips virtual-security-domain office countermeasure record

Total 3 times countermeasure, current 3 countermeasure record in virtual-security-domain office

Reason: Att - attack; Ass - associated; Black - blacklist;

Class - classification; Manu - manual;

MAC address	Type	Reason	Countermeasure AP	Radio ID	Time
1000-0000-00e3	AP	Manu	fatap	1	2020-05-03/09:32:01
1000-0000-00e4	AP	Manu	fatap	1	2020-05-03/09:32:11
2000-0000-f282	Client	Black	fatap	1	2020-05-03/09:31:56

表 2-3 コマンド出力

フィールド	説明
Total *number* times countermeasure, current *number* countermeasure record in virtual-security-domain *name*	成功した対策の数です。このフィールドには、最大1024件の対策レコードを表示できます。
MAC Address	WIPSが対策を講じた無線装置のMACアドレスです。
Type	ワイヤレス装置のタイプ:APまたはクライアントです。
Reason	WIPSがワイヤレス装置対策を行う理由: • **Att**－WIPSは装置が攻撃者であるために対策を講じています。 • **Class** — WIPSは装置に対して装置型をベースにした対抗策をとっています。 • **Manu** — WIPSは装置アドレスに基づいてMACへの対抗策をとります。
Countermeasure AP	無線装置対策センサの名称です。
Radio ID	無線装置対策を行うセンサの無線IDです。
Time	無線装置対策をセンサに通知する時間です。

関連コマンド

reset wips virtual-security-domain countermeasure record

2.1.63 display wips virtual-security-domain device

Syntax

display wips virtual-security-domain *vsd-name* **device** [**ap** [**ad-hoc | authorized | external | mesh | misconfigured | potential-authorized | potential-external | potential-rogue | rogue | uncategorized**] **| client** [[**dissociative-client**] **|** [**authorized | misassociation | unauthorized | uncategorized**]] **| mac-address** *mac-address*] [**verbose**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 無線装置の情報を表示します。

ap: AP の情報を表示します。

ad-hoc: アドホックモードで動作する AP に関する情報を表示します。

authorized: 許可 AP に関する情報を表示します。

external: 外部 AP に関する情報を表示します。

mesh: MP に関する情報を表示します。

misconfigured: 間違って設定された AP に関する情報を表示します。

potential-authorized: 潜在的に許可された AP に関する情報を表示します。

potential-rogue: 潜在的な不正 AP に関する情報を表示します。

potential-external: 潜在的外部 AP に関する情報を表示します。

rogue: 不正な AP に関する情報を表示します。

uncategorized: 分類されていない AP に関する情報を表示します。

client: クライアント情報を表示します。

dissociative-client: 紐付けられていないクライアント情報を表示します。

authorized: 許可クライアントに関する情報を表示します。

misassociation: 間違って紐付けられたクライアントに関する情報を表示します。

unauthorized: 未許可クライアントに関する情報を表示します。

uncategorized: 分類されていないクライアントに関する情報を表示します。

mac-address *mac-address*: 特定の無線装置に関する情報を表示します。*mac-address* 引数は無線装置の MAC アドレスを表し、H-H-H 形式です。

verbose: 詳細な装置情報を表示します。

説明

display wips virtual-security-domain device コマンドは VSD で検出された無線装置に関する情報を表示します。

例

VSD **office** で検出された無線装置に関する情報を表示します。

<AP> display wips virtual-security-domain office device

```
Total 3 detected devices in virtual-security-domain office

Class: Auth - authorization; Ext - external; Mis - mistake;
      Unauth - unauthorized; Uncate - uncategorized;
      (A) - associate; (C) - config; (P) - potential;
      Ad-hoc; Mesh

MAC address    Type   Class    Duration    Sensors Channel Status
1000-0000-0000 AP     Ext(P)   00h 10m 46s 1       11      Active
1000-0000-0001 AP     Ext(P)   00h 10m 46s 1       6       Active
1000-0000-0002 AP     Ext(P)   00h 10m 46s 1       1       Active
```

表 2-4 コマンド出力

フィールド	説明
Type	無線装置タイプ： AP、Client、またはMesh
Class	無線装置のカテゴリ
Duration	無線装置が現在の状態に移行してからの期間
Sensors	無線装置を検出したセンサの数
Channel	直近で無線装置が検出されたチャネル
Status	APもしくはクライアントの状態 • **Active**－APもしくはクライアントはアクティブです。 • **Inactive**－APもしくはクライアントは非アクティブです。

VSD **a** で検出された無線装置に関する詳細な情報を表示します。

<AP> display wips virtual-security-domain a device verbose

```
Total 2 detected devices in virtual-security-domain a
```

```
 AP: 1000-0000-0000
   Mesh Neighbor: None
   Classification: Mis(C)
   Severity level: 0
   Classify way: Auto
   Status: Active
   Status duration: 00h 27m 57s
   Vendor: Not found
   SSID: service
   Radio type: 802.11g
   Countermeasuring: No
   Security: None
   Encryption method: None
   Authentication method: None
   Broadcast SSID: Yes
   QoS supported: No
   Ad-hoc: No
   Beacon interval: 100 TU
   Up duration: 00h 27m 57s
Channel band-width supported: 20MHZ
   Hotspot AP: No
   Soft AP: No
   Honeypot AP: No
   Total number of reported sensors: 1
     Sensor 1:
       Sensor ID: 1
       Sensor name: fatap
       Radio ID: 1
       RSSI: 15
       Channel: 64
       First reported time: 2014-06-03/09:05:51
       Last reported time: 2014-06-03/09:05:51
   Total number of associated clients: 1
     01: 2000-0000-0000
Client: 2000-0000-0000
  Last reported associated AP: 1000-0000-0000
  Classification: Uncate
  Severity level: 0
  Classify way: Auto
  Dissociative status: No
  Status: Active
  Status duration: 00h 00m 02s
```

```
Vendor: Not found
Radio type: 802.11a
40MHz intolerance: No
Countermeasuring: No
Man in the middle: No
Total number of reported sensors: 1
  Sensor 1:
    Sensor ID: 1
    Sensor name: fatap
    Radio ID: 1
    RSSI: 50
    Channel: 64
    First reported time: 2014-06-03/14:52:56
    Last reported time: 2014-06-03/14:52:56
    Reported associated AP: 1000-0000-0000
```

表 2-5 コマンド出力

フィールド	説明
AP	APのMACアドレス
Mesh Neighbor	メッシュAPのネイバのMACアドレス
Client	クライアントのMACアドレス
Last reported associated AP	クライアントが直近で報告した、紐付けられたAPのMACアドレス

フィールド	説明

Classification	APもしくはクライアントのカテゴリ
	• APカテゴリオプション
	  • ad_hoc
	  • authorized
	  • rogue
	  • misconfigured
	  • external
	  • potential-authorized
	  • potential-rogue
	  • potential-external
	  • uncategorized
	• クライアントカテゴリオプション
	  • authorized
	  • unauthorized
	  • misassociated
	  • uncategorized

Severity level	装置の重大度レベル
Classify way	APもしくはクライアント分類方法 • **Manual**－手動分類 • **Invalid OUI**－無効なOUIリストに追加 • **Block List**－禁止装置リストに追加 • **Trust List**－許可装置リストに追加 • **User Define**－ユーザが定義した分類 • **Auto**－自動分類
Dissociative status	クライアントが紐付けられたものではないかどうかをあらわします。
Status	APもしくはクライアントの状態 • **Active**－APもしくはクライアントはアクティブです。 • **Inactive**－APもしくはクライアントは非アクティブです。
Status duration	無線装置が現在の状態に移行してからの期間
Vendor	装置のOUI。装置のOUIが、インポートされたOUIと一致する場合、このフィールドは装置のOUIを表示します。装置にOUIが設定されていない場合、あるいは装置のOUIが、インポートされたいずれのOUIとも一致しない場合、このフィールドは**Not found**を表示します。

フィールド	説明
SSID	APに提供された無線装置のSSID
Radio Type	無線装置の無線モード
40MHz intolerance	クライアントが40MHz帯をサポートするかどうかをあらわします。
Countermeasuring	WIPSが無線装置に対策を講じるかをあらわします。 ● No ● Yes
Man in the middle	MITM攻撃を検出するかどうかをあらわします。
Security	セキュリティ方式。 ● None ● WEP ● WPA ● WPA2
Encryption method	データ暗号方式。 ● TKIP ● CCMP ● WEP ● None
Authentication method	認証方式。 ● None ● PSK ● 802.1X ● Others－PSK認証と802.1X認証以外の認証方式
Broadcast SSID	APがSSIDをブロードキャストするかどうかをあらわします。APがSSIDをブロードキャストしない場合、このフィールドは何も表示しません。
QoS supported	無線装置がQoSをサポートするかどうかをあらわします。
Ad-hoc	無線装置がアドホックモードかどうかをあらわします。
Beacon interval	TUにおけるビーコン間隔です。1つのTUは1024マイクロ秒に等しいです。
Channel band-width supported	サポートされたチャネル帯域幅モード ● 20/40/80MHZ ● 20/40MHz ● 20MHz

フィールド	説明
Hotspot AP	APがホットスポット攻撃APであるかどうかをあらわします。
Soft AP	APがソフトAPであるかどうかをあらわします。
Honeypot AP	APがハニーポットAPであるかどうかをあらわします。
Sensor n	無線装置を検出したセンサです。n はシステムに割り当てられたIDをあらわします。
Channel	センサが直近で無線装置を検出したチャネルです。
First reported time	センサが最初に無線装置を検出した時間です。
Last reported time	センサが直近で無線装置を検出した時間です。
n: H-H-H	APに紐付けられたMACアドレスです。n はシステムに割り当てられたIDをあらわします。
Reported associated AP	センサが報告した、紐付けられたAPのMACアドレスです。

関連コマンド

reset wips virtual-security-domain device

2.1.64 embedded-oui-classify enable

Syntax

embedded-oui-classify enable

デフォルト

設定なし

View

Device category view

定義済みユーザロール

network-admin

説明

flood association-request コマンドは WIPS OUI ライブラリの内蔵 OUI に基づいてデバイスを分類します。

例

装置分類ポリシー**home** の WIPS OUI ライブラリの組み込み OUI に基づく装置分類を有効にします。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] embedded-oui-classify enable

関連コマンド

reset wips embedded-oui

2.1.65 export oui

Syntax

export oui *file-name*

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: 設定ファイルを名前で指定します。大文字と小文字は区別されず、1~255 文字の文字列で指定します。バックスラッシュ(¥)、スラッシュ(/)、コロン (:) 、アスタリスク(*)、疑問符 (?)、クオーテーションマーク (")、左山括弧 (<) 、右山括弧(>) 、縦棒(|)は使用できません。

説明

export oui コマンドは OUI ライブラリ内のすべての OUI を OUI 設定ファイルにエクスポートします。

このコマンドは、埋め込み OUI とインポートされた OUI を含むすべての OUI をエクスポートします。

OUI は次の形式でエクスポートされます。

```
000FE2 (base 16) New H3C Technologies Co., Ltd..
```

例

OUI ライブラリ内のすべての OUI を構成ファイル **OUIInfo** にエクスポートします。

<AP> system-view

[AP] wips

[AP-wips] export oui OUIInfo

関連コマンド

- i**mport oui**
- **reset wips embedded-oui**

2.1.66 flood association-request

Syntax

flood association-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood association-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 紐付け要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が紐付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に紐付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 紐付け要求フラッド攻撃アラームを引き起こす紐付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood association-request コマンドは紐付け要求フラッド攻撃検出を設定します。

undo flood association-request コマンドはデフォルトに戻します。

例

紐付け要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood association-request interval 100 threshold 100 quiet 360

2.1.67 flood authentication

Syntax

flood authentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood authentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 認証要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証要求フラッド攻撃アラームを引き起こす認証要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood authentication コマンドは認証要求フラッド攻撃検出を設定します。

undo flood authentication コマンドはデフォルトに戻します。

例

認証要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood authentication interval 100 threshold 100 quiet 360

2.1.68 flood beacon

Syntax

flood beacon [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood beacon

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ビーコンフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がビーコンフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にビーコンフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ビーコンフラッド攻撃アラームを引き起こすビーコンフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood beacon コマンドはビーコンフラッド攻撃検出を設定します。

undo flood beacon コマンドはデフォルトに戻します。

例

ビーコンフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood beacon interval 100 threshold 100 quiet 360

2.1.69 flood block-ack

Syntax

flood block-ack [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood block-ack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ブロックアクトフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がブロックアクトフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にブロックアクトフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ブロックアクトフラッド攻撃アラームを引き起こすブロックアクトフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood block-ack コマンドはブロックアクトフラッド攻撃検出を設定します。

undo flood block-ack コマンドはデフォルトに戻します。

例

ブロックアクトフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood block-ack interval 100 threshold 100 quiet 360

2.1.70 flood cts

Syntax

flood cts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood cts

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: CTS フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が CTS フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に CTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: CTS フラッド攻撃アラームを引き起こす CTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood cts コマンドは CTS フラッド攻撃検出を設定します。

undo flood cts コマンドはデフォルトに戻します。

例

CTS フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood cts interval 100 threshold 100 quiet 360

2.1.71 flood deauthentication

Syntax

flood deauthentication [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood deauthentication

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 認証取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が認証取り消しフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に認証取り消しフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 認証取り消しフラッド攻撃アラームを引き起こす認証取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood deauthentication コマンドは認証取り消しフラッド攻撃検出を設定します。

undo flood deauthentication コマンドはデフォルトに戻します。

例

認証取り消しフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood deauthentication interval 100 threshold 100 quiet 360

2.1.72 flood disassociation

Syntax

flood disassociation [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood disassociation

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 紐付け取り消しフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が紐付け取り消しフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に紐付け取り消しフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 紐付け取り消しフラッド攻撃アラームを引き起こす紐付け取り消しフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood disassociation コマンドは紐付け取り消しフラッド攻撃検出を設定します。

undo flood disassociation コマンドはデフォルトに戻します。

例

紐付け取り消しフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood disassociation interval 100 threshold 100 quiet 360

2.1.73 flood eap-failure

Syntax

flood eap-failure [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-failure

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAP 失敗フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAP 失敗フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAP 失敗フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAP 失敗フラッド攻撃アラームを引き起こす EAP 失敗フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eap-failure コマンドは EAP 失敗フラッド攻撃検出を設定します。

undo flood eap-failure コマンドはデフォルトに戻します。

例

EAP 失敗フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood eap-failure interval 100 threshold 100 quiet 360

2.1.74 flood eapol-logoff

Syntax

flood eapol-logoff [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-logoff

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAPOL ログオフフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL ログオフフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL ログオフフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL ログオフフラッド攻撃アラームを引き起こす EAPOL ログオフフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-logoff コマンドは EAPOL ログオフフラッド攻撃検出を設定します。

undo flood eapol-logoff コマンドはデフォルトに戻します。

例

EAPOL ログオフフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood eapol-logoff interval 100 threshold 100 quiet 360

2.1.75 flood eapol-start

Syntax

flood eapol-start [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eapol-start

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAPOL スタートフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAPOL スタートフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAPOL スタートフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAPOL スタートフラッド攻撃アラームを引き起こす EAPOL スタートフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eapol-start コマンドは EAPOL スタートフラッド攻撃検出を設定します。

undo flood eapol-start コマンドはデフォルトに戻します。

例

EAPOL スタートフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood eapol-start interval 100 threshold 100 quiet 360

2.1.76 flood eap-success

Syntax

flood eap-success [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood eap-success

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: EAP 成功フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が EAP 成功フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に EAP 成功フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: EAP 成功フラッド攻撃アラームを引き起こす EAP 成功フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood eap-success コマンドは EAP 成功フラッド攻撃検出を設定します。

undo flood eap-success コマンドはデフォルトに戻します。

例

EAP 成功フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood eap-success interval 100 threshold 100 quiet 360

2.1.77 flood null-data

Syntax

flood null-data [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood null-data

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: ヌルデータフレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がヌルデータフラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にヌルデータフラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: ヌルデータフラッド攻撃アラームを引き起こすヌルデータフレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood null-data コマンドはヌルデータフラッド攻撃検出を設定します。

undo flood null-data コマンドはデフォルトに戻します。

例

ヌルデータフラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood null-data interval 100 threshold 100 quiet 360

2.1.78 flood probe-request

Syntax

flood probe-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood probe-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: プローブ要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS がプローブ要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にプローブ要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: プローブ要求フラッド攻撃アラームを引き起こすプローブ要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood probe-request コマンドはプローブ要求フラッド攻撃検出を設定します。

undo flood probe-request コマンドはデフォルトに戻します。

例

プローブ要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood probe-request interval 100 threshold 100 quiet 360

2.1.79 flood reassociation-request

Syntax

flood reassociation-request [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood reassociation-request

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: 再紐付け要求フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が再紐付け要求フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に再紐付け要求フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: 再紐付け要求フラッド攻撃アラームを引き起こす再紐付け要求フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood reassociation-request コマンドは再紐付け要求フラッド攻撃検出を設定します。

undo flood reassociation-request コマンドはデフォルトに戻します。

例

再紐付け要求フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood reassociation-request interval 100 threshold 100 quiet 360

2.1.80 flood rts

Syntax

flood rts [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *

undo flood rts

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: RTS フレームのための統計値収集間隔を指定します。値の範囲は 1～3600 秒です。デフォルトの収集間隔は 60 秒です。

quiet *quiet-value*: WIPS が RTS フラッド攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に RTS フラッド攻撃を検出してもアラームを引き起こしません。

threshold *threshold-value*: RTS フラッド攻撃アラームを引き起こす RTS フレーム数を指定します。*threshold-value* 引数の値の範囲は 1～100000 です。デフォルト値は 50 です。

説明

flood rts コマンドは RTS フラッド攻撃検出を設定します。

undo flood rts コマンドはデフォルトに戻します。

例

RTS フラッド攻撃検出を有効にします。*interval-value*、*quiet-value*、*threshold-value* の値をそれぞれ、100、360、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] flood rts interval 100 threshold 100 quiet 360

2.1.81 frame-type

Syntax

frame-type { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }

undo frame-type

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

control: 制御フレームと整合します。

data: データフレームと整合します。

management: 管理フレームと整合します。

frame-subtype: フレームサブタイプを指定します。

association-request: 紐付け要求フレームと整合します。

association-response: 紐付け応答フレームと整合します。

authentication: 認証フレームと整合します。

beacon: ビーコンフレームと整合します。

deauthentication: 認証取り消しフレームと整合します。

disassociation: 紐付け取り消しフレームと整合します。

probe-request: プローブ要求フレームと整合します。

説明

frame-type コマンドはフレームのフレームタイプと整合するためにサブ署名を設定します。

undo frame-type コマンドはデフォルトに戻します。

例

データフレームと一致するように signature 1 に対してサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] frame-type data

2.1.82 honeypot-ap

Syntax

honeypot-ap [**similarity** *similarity-value* | **quiet** *quiet-value*] *

undo honeypot-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

similarity *similarity-value*: ハニーポット AP アラームを引き起こす類似のしきい値を指定します。値の範囲は 70～100%です。デフォルト値は 80%です。AP の SSID と適合 AP の SSID との間の類似点がしきい値に達すると、AP はハニーポット AP とみなされます。

quiet *quiet-value*: WIPS がハニーポット AP 検出アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット AP を検出してもアラームを引き起こしません。

説明

honeypot-ap コマンドはハニーポット AP 検出を設定します。

undo honeypot-ap コマンドはハニーポット AP 検出を無効にします。

例

ハニーポット AP 検出を有効にします。類似のしきい値と遅延時間をそれぞれ、90%、10 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] honeypot-ap similarity 90 quiet 10

2.1.83 hotspot-attack

Syntax

hotspot-attack [**quiet** *quiet-value*]

undo hotspot-attack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がハニーポット攻撃アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にハニーポット攻撃を検出してもアラームを引き起こしません。

説明

hotspot-attack コマンドはハニーポット攻撃検出を設定します。

undo hotspot-attack コマンドはハニーポット攻撃検出を無効にします。

例

ハニーポット攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] hotspot-attack quiet 100

2.1.84 hotspot ssid

Syntax

hotspot ssid *ssid-name*

undo hotspot ssid { *ssid-name* | **all** }

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

ssid-name: 名前で SSID を指定します。1 文字から 32 文字の文字列で、大文字と小文字が区別されます。

all: すべての SSID を指定します。

説明

hotspot ssid コマンドはホットスポット SSID として SSID を指定します。

undo hotspot ssid コマンドは指定された 1 つまたはすべてのホットスポット SSID を削除します。

デフォルトでは、装置にはホットスポット SSID が組み込まれています。組み込みのホットスポット SSID は削除できません。SSID をホットスポット SSID として指定するには、次のいずれかの操作を行います。

- 設定ファイルの SSID 設定を編集し、**import hotspot** コマンドを実行して、変更した設定ファイルを装置にインポートします。この方法を使用して、複数の SSID をホットスポット SSID として指定できます。
- **hotspot ssid** コマンドを実行して、ホットスポット SSID として SSID を指定します。

例

ホットスポット SSID に、SSID **cmcc** を指定します。

<AP> system-view

[AP] wips

[AP-wips] hotspot ssid cmcc

関連コマンド

import hotspot

2.1.85 ht-40mhz-intolerance

Syntax

ht-40mhz-intolerance [**quiet** *quiet-value*]

undo ht-greenfield

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が 40MHz の帯域幅モードを使用禁止にしたクライアントを検出するアラームを開始した後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を設定します。

undo ht-40mhz-intolerance コマンドは 40MHz の帯域幅モードを使用禁止にしたクライアントの検出を無効にします。

例

40MHz の帯域幅モードを使用禁止にしたクライアント検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ht-40mhz-intolerance quiet 100

2.1.86 ht-greenfield

Syntax

ht-greenfield [**quiet** *quiet-value*]

undo ht-greenfield

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が HT グリーンフィールド AP 検出アラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に HT グリーンフィールド AP を検出してもアラームを引き起こしません。

説明

ht-greenfield コマンドは HT グリーンフィールド検出を設定します。

undo ht-greenfield コマンドは HT グリーンフィールド検出を無効にします。

例

HT グリーンフィールド AP 検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] ht-greenfield quiet 100

2.1.87 ignorelist

Syntax

ignorelist mac-address *mac-address*

undo ignorelist mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mac-address: MAC アドレスを H-H-H 形式で指定します。

all: アラームを無視する装置リスト内のすべてのすべての MAC アドレスを指定します。

説明

ignorelist コマンドはアラームを無視する装置リストに MAC アドレスを追加します。

undo ignorelist コマンドはアラームを無視する装置リストから特定の、もしくはすべての MAC アドレスを削除します。

WIPS は、アラームを無視する装置リスト内の無線装置のみを監視しますが、アラームはあげません。

例

アラームを無視する装置リストに MAC アドレス **2a11-1fa1-1311** を追加します。

<AP> system-view

[AP] wips

[AP-wips] ignorelist mac-address 2a11-1fa1-1311

2.1.88 import hotspot

Syntax

import hotspot *file-name*

undo import hotspot

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import hotspot コマンドはコンフィグレーションファイルからホットスポットをインポートします。

undo import hotspot コマンドはコンフィグレーションファイルを削除します。

1 つのコンフィグレーションファイルからのみホットスポットをインポートできます。

例

コンフィグレーションファイル **hotspot_cfg** からホットスポットをインポートします。

<AP> system-view

[AP] wips

[AP-wips] import hotspot hotspot_cfg

2.1.89 import oui

Syntax

import oui *file-name*

undo import oui

デフォルト

インポートなし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

file-name: コンフィグレーションファイルの名前を指定します。大文字と小文字は区別しません。文字数は 1～255 文字です。バックスラッシュ、スラッシュ（/）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、クォーテーションマーク（"）、左括弧（<）、右括弧（>）、縦棒（|）は使用できません。

説明

import oui コマンドはコンフィグレーションファイルから OUI をインポートします。

undo import oui コマンドはコンフィグレーションを削除します。

IEEE ウェブサイトからコンフィグレーションファイルをダウンロードできます。

1 つのコンフィグレーションファイルからのみ OUI をインポートできます。

例

コンフィグレーションファイル **oui_import_cfg** から OUI をインポートします。

<AP> system-view

[AP] wips

[AP-wips] import oui oui_import_cfg

関連コマンド

invalid-oui-classify illegal

2.1.90 invalid-oui-classify illegal

Syntax

invalid-oui-classify illegal

undo invalid-oui-classify

デフォルト

無効

View

Classification policy view

定義済みユーザロール

network-admin

説明

invalid-oui-classify illegal コマンドは無効な OUI で装置を不正な装置として分類するように WIPS を有効にします

undo invalid-oui-classify コマンドはデフォルトに戻します。

例

無効な OUI で装置を不正な装置として分類するように WIPS を設定します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] invalid-oui-classify illegal

関連コマンド

import oui

2.1.91 mac-address

Syntax

mac-address { **bssid** | **destination** | **source** } *mac-address*

undo mac-address

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

bssid: 指定された BSSID と整合します。

destination: 指定された送信元 MAC アドレスと整合します。

source: 指定された送信元 MAC アドレスと整合します。

mac-address: MAC アドレスを H-H-H 形式で指定します。

説明

mac-address コマンドはフレームが送信元 MAC アドレスと整合するようにサブ署名を設定します。

undo mac-address コマンドはデフォルトに戻します。

例

フレームが送信元 MAC アドレス **000f-e201-0101** と整合するように signature 1 に対してサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] mac-address source 000f-e201-0101

2.1.92 malformed duplicated-ie

Syntax

malformed duplicated-ie [**quiet** *quiet-value*]

undo malformed duplicated-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が複製された IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に複製された IE を検出してもアラームを引き起こしません。

説明

malformed duplicated-ie コマンドは複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。

undo malformed duplicated-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。複製された IE をパケットが持つ場合、WIPS はパケットを異常とみなします。この検出はベンダに定義された IE には適用できません。

例

複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed duplicated-ie quiet 360

2.1.93 malformed fata-jack

Syntax

malformed fata-jack [**quiet** *quiet-value*]

undo malformed fata-jack

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が FATA ジャック異常パケットアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に FATA ジャック異常パケットを検出してもアラームを引き起こしません。

説明

malformed fata-jack コマンドは FATA ジャック異常パケットを検出するように、WIPS を有効にします。

undo malformed fata-jack コマンドはデフォルトに戻します。

この機能は認証フレームに適用できます。認証アルゴリズム番号の値が 2 である場合、WIPS は認証フレームを異常とみなします。

例

複製された IE を伴った異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed fata-jack quiet 360

2.1.94 malformed illegal-ibss-ess

Syntax

malformed illegal-ibss-ess [**quiet** *quiet-value*]

undo malformed illegal-ibss-ess

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常 IBSS および ESS 設定のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常 IBSS および ESS 設定を検出してもアラームを引き起こしません。

説明

malformed illegal-ibss-ess コマンドは異常 IBSS および ESS 設定をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed illegal-ibss-ess コマンドはデフォルトに戻します。

この機能はビーコンフレームおよびプローブ応答フレームに適用できます。IBSS と ESS がフレーム内でともに 1 に設定されている場合、WIPS はフレームを異常とみなします。

例

異常 IBSS および ESS 設定をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed illegal-ibss-ess quiet 360

2.1.95 malformed invalid-address-combination

Syntax

malformed invalid-address-combination [**quiet** *quiet-value*]

undo malformed invalid-address-combination

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な送信元アドレスのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な送信元アドレスを検出してもアラームを引き起こしません。

説明

malformed invalid-address-combination コマンドは無効な送信元アドレスをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-address-combination コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- フレームの TO DS が 1 の場合。（フレームがクライアントにより AP に送信されたことを示します）
- フレームの送信元 MAC アドレスがマルチキャストアドレスもしくはブロードキャストアドレスの場合。

例

無効な送信元アドレスをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-address-combination quiet 360

2.1.96 malformed invalid-assoc-req

Syntax

malformed invalid-assoc-req [**quiet** *quiet-value*]

undo malformed invalid-assoc-req

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常紐付け要求フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常紐付け要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-assoc-req コマンドは異常紐付け要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-assoc-req コマンドはデフォルトに戻します。

この機能は紐付け要求フレームに適用できます。フレーム内の SSID 長が 0 である場合、WIPS はフレームを異常とみなします。

例

異常紐付け要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-assoc-req quiet 360

2.1.97 malformed invalid-auth

Syntax

malformed invalid-auth [**quiet** *quiet-value*]

undo malformed invalid-auth

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常認証要求フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常認証要求フレームを検出してもアラームを引き起こしません。

説明

malformed invalid-auth コマンドは異常認証要求フレームを検出するように、WIPS を有効にします。

undo malformed invalid-auth コマンドはデフォルトに戻します。

この機能は認証要求フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- 認証アルゴリズム番号が 802.11 プロトコルと一致せず、3 より大きい場合。
- 認証トランザクションシーケンス番号が 1 であり、状態コードが 0 で無い場合。（認証トランザクションシーケンス番号は、クライアントと AP 間の認証処理を示します。）
- 認証トランザクションシーケンス番号が 4 より大きい場合。

例

異常認証要求フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-auth quiet 360

2.1.98 malformed invalid-deauth-code

Syntax

malformed invalid-deauth-code [**quiet** *quiet-value*]

undo malformed invalid-deauth-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な認証取り消しコードのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な認証取り消しコードを検出してもアラームを引き起こしません。

説明

malformed invalid-deauth-code コマンドは無効な認証取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-deauth-code コマンドはデフォルトに戻します。

この機能は認証取り消しフレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを異常とみなします。

例

無効な認証取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-deauth-code quiet 360

2.1.99 malformed invalid-disassoc-code

Syntax

malformed invalid-disassoc-code [**quiet** *quiet-value*]

undo malformed invalid-disassoc-code

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な紐付け取り消しコードのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な紐付け取り消しコードを検出してもアラームを引き起こしません。

説明

malformed invalid-disassoc-code コマンドは無効な紐付け取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-disassoc-code コマンドはデフォルトに戻します。

この機能は紐付け取り消しフレームに適用できます。フレーム内の原因コードが 0、もしくは 67～65535 の範囲内である場合、WIPS はフレームを異常とみなします。

例

無効な紐付け取り消しコードをもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-disassoc-code quiet 360

2.1.100 malformed invalid-ht-ie

Syntax

malformed invalid-ht-ie [**quiet** *quiet-value*]

undo malformed invalid-ht-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常 HT IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常 HT IE を検出してもアラームを引き起こしません。

説明

malformed invalid-ht-ie コマンドは異常 HT IE をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ht-ie コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ応答フレーム、紐付け応答フレーム、再紐付け応答フレームに適用できます。WIPS は以下の条件において、フレームを異常とみなします。

- HT ケーパビリティ IE の SM 電力節約値が 2 である場合。
- HT オペレーション IE のセカンダリチャネルオフセット値が 2 である場合。

例

異常 HT IE をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-ht-ie quiet 360

2.1.101 malformed invalid-ie-length

Syntax

malformed invalid-ie-length [**quiet** *quiet-value*]

undo malformed invalid-ie-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効な IE 長のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効な IE 長を検出してもアラームを引き起こしません。

説明

malformed invalid-ie-length コマンドは無効な IE 長をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-ie-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE 長が 802.11 プロトコルと一致しない場合、WIPS はフレームを異常とみなします。

例

無効な IE 長をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-ie-length quiet 360

2.1.102 malformed invalid-pkt-length

Syntax

malformed invalid-pkt-length [**quiet** *quiet-value*]

undo malformed invalid-pkt-length

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無効なパケット長のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に無効なパケット長を検出してもアラームを引き起こしません。

説明

malformed invalid-pkt-length コマンドは無効なパケット長をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed invalid-pkt-length コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。パケットペイロード解析後に IE の残存長が 0 で無い場合、WIPS はフレームを異常とみなします。

例

無効なパケット長をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed invalid-pkt-length quiet 360

2.1.103 malformed large-duration

Syntax

malformed large-duration [**quiet** *quiet-value* | **threshold** *value*]

undo malformed large-duration

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな期間のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな期間を検出してもアラームを引き起こしません。

threshold *threshold-value*: WIPS がオーバーサイズな期間を判断し、アラームをあげるために、期間のサイズを指定します。*value* 引数の値の範囲は 1〜32767 です。デフォルト値は 5000 です。

説明

malformed large-duration コマンドはオーバーサイズな期間をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed large-duration コマンドはデフォルトに戻します。

この機能はユニキャスト管理フレーム、ユニキャストデータフレーム、RTS フレーム、CTS フレーム、ACK フレームに適用できます。フレーム内の期間の値が指定されたしきい値より大きい場合、WIPS はフレームを異常とみなします。

例

オーバーサイズな期間をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed large-duration quiet 360

2.1.104 malformed null-probe-resp

Syntax

malformed null-probe-resp [**quiet** *quiet-value*]

undo malformed null-probe-resp

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が異常プローブ応答フレームのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に異常プローブ応答フレームを検出してもアラームを引き起こしません。

説明

malformed null-probe-resp コマンドは異常プローブ応答フレームを検出するように、WIPS を有効にします。

undo malformed null-probe-resp コマンドはデフォルトに戻します。

この機能はプローブ応答フレームに適用できます。フレームがメッシュフレームでなく、SSID 長が 0 である場合、WIPS はフレームを異常とみなし、パケットは異常パケットとみなします。

例

異常プローブ応答フレームを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed null-probe-resp quiet 360

2.1.105 malformed overflow-eapol-key

Syntax

malformed overflow-eapol-key [**quiet** *quiet-value*]

undo malformed overflow-eapol-key

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな EAPOL 鍵のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな EAPOL 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-eapol-key コマンドはオーバーサイズな EAPOL 鍵をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed overflow-eapol-key コマンドはデフォルトに戻します。

この機能は EAPOL 鍵フレームに適用できます。フレーム内の TO DS が 1 で、鍵長が 0 より大きい場合、WIPS はフレームを異常とみなします。悪意ある EAPOL 鍵フレームにより DOS 攻撃を受ける恐れがあります。

例

オーバーサイズな EAPOL 鍵をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed overflow-eapol-key quiet 360

2.1.106 malformed overflow-ssid

Syntax

malformed overflow-ssid [**quiet** *quiet-value*]

undo malformed overflow-ssid

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がオーバーサイズな SSID のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にオーバーサイズな SSID 鍵を検出してもアラームを引き起こしません。

説明

malformed overflow-ssid コマンドはオーバーサイズな SSID をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed overflow-ssid コマンドはデフォルトに戻します。

この機能はビーコンフレーム、プローブ要求フレーム、プローブ応答フレーム、紐付け要求フレームに適用できます。フレーム内の SSID 長が 32 より大きく、802.11 プロトコルに一致していない場合、WIPS はフレームを異常とみなします。

例

オーバーサイズな SSID をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed overflow-ssid quiet 360

2.1.107 malformed redundant-ie

Syntax

malformed redundant-ie [**quiet** *quiet-value*]

undo malformed redundant-ie

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が冗長な IE のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に冗長な IE を検出してもアラームを引き起こしません。

説明

malformed redundant-ie コマンドは冗長な IE をもつ異常パケットを検出するように、WIPS を有効にします。

undo malformed redundant-ie コマンドはデフォルトに戻します。

この機能はすべての管理フレームに適用できます。フレーム内の IE がフレームにとって必要な IE でも予備の IE でもない場合、WIPS はフレームを異常とみなします。

例

冗長な IE をもつ異常パケットを検出するように、WIPS を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] malformed redundant-ie quiet 360

2.1.108 man-in-the-middle

Syntax

man-in-the-middle [**quiet** *quiet-value*]

undo man-in-the-middle

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が MITM（Man-In-The-Middle）攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に MITM 攻撃を検出してもアラームを引き起こしません。

説明

man-in-the-middle コマンドは MITM 攻撃検出を有効にします。

undo man-in-the-middle コマンドは MITM 攻撃検出を無効にします。

MITM 攻撃検出を有効にする前にハニーポット AP 検出を有効にしてください。

例

MITM 攻撃検出を有効にします。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] honeypot-ap

[AP-wips-dtc-home] man-in-the-middle

2.1.109 manual-classify mac-address

Syntax

manual-classify mac-address *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }

undo manual-classify mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: AP の MAC アドレスを H-H-H 形式で指定します。

authorized-ap: AP を許可された AP として指定します。

external-ap: AP を外部 AP として指定します。

misconfigured-ap: AP を間違って設定された AP として指定します。

rogue-ap: AP を不正な AP として指定します。

all: すべての AP を指定します。

説明

manual-classify mac-address コマンドは AP に対してカテゴリを設定します。

undo manual-classify mac-address コマンドはデフォルトに戻します。

例

MAC アドレスが 000f-00e2-0001 の AP を許可された AP として設定します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] manual-classify mac-address 000f-00e2-0001 authorized-ap

2.1.110 match all (AP classification rule view)

Syntax

match all

undo match all

デフォルト

AP 分類ルールの基準は、論理 OR 関係にあります。AP 分類ルールの基準のいずれかに一致する場合、AP は AP 分類ルールに一致します。

View

AP classification rule view

定義済みユーザロール

network-admin

説明

match all コマンドは AP 分類ルールの基準が論理 AND 関係になるように設定します。

undo match all コマンドはデフォルトに戻します。

例

AP 分類ルール 1 の基準を論理 AND 関係にするように設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] match all

2.1.111 match all (signature view)

yntax

match all

undo match all

デフォルト

副署名は論理 OR 関係にあります。パケットは、署名のいずれかの副署名と一致する場合、署名と一致します。

View

Signature view

定義済みユーザロール

network-admin

説明

match all コマンドはサブ署名が論理 AND 関係になるように設定します。

undo match all コマンドはデフォルトに戻します。

例

署名 1 の副署名を論理 AND 関係にするように設定します

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[wips-sig-rule-1] match all

関連コマンド

- **frame-type**
- **mac-address**
- **pattern**
- **seq-number**
- **ssid (signature rule view)**
- **ssid-length**

2.1.112 omerta

Syntax

omerta [**quiet** *quiet-value*]

undo omerta

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Omerta 攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に Omerta 攻撃を検出してもアラームを引き起こしません。

説明

omerta コマンドは Omerta 攻撃検出を有効にします。

undo omerta コマンドは Omerta 攻撃検出を無効にします。

例

Omerta 攻撃検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] omerta quiet 100

2.1.113 oui

Syntax

oui *oui-info*

undo oui

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

oui-info: OUI 情報を XXXXXX 形式で指定します。大文字と小文字を区別しません。16 進数で指定します。

説明

oui コマンドは AP の OUI 情報と整合するように AP 分類ルールを設定します。

undo oui コマンドはデフォルトに戻します。

例

AP を OUI **000fe4** と整合するために AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] oui 000fe4

2.1.114 pattern

Syntax

pattern *pattern-number* **offset** *offset-value* **mask** *mask value1* [**to** *value2*] [**from-payload**]

undo pattern { *pattern-number* | **all** }

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

pattern-number: 0〜65535 の範囲の数字で指定されたフレームのビットと一致するサブ署名を指定します。

offset *offset-value*: 指定されたビットから参照ビットまでのオフセットを指定します。*offset-value* 引数の値の範囲は 0〜2346 ビットです。参照ビットは、フレームヘッド（デフォルト）もしくはフレームペイロードの最初のビットになることができます。

mask *mask*: 指定されたビットで AND 演算に使用される 2 バイトマスクを指定します。マスクは 16 進数形式です。マスクの値の範囲は 0〜ffff です。

value1 [**to** *value2*]: ビット数の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0〜65535 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

from-payload: 参照ビットとしてフレームペイロードの最初のビットを指定します。このキーワードを指定しない場合、フレームヘッドの最初のビットは参照ビットになります。

説明

pattern コマンドは指定されたフレームのビットと整合するようにサブ署名を設定します。

undo pattern コマンドはデフォルトに戻します。

例

フレームヘッドの第 2 ビットと第 3 ビットが整合するようにサブ署名を設定します。フレームの第 2 ビットと第 3 ビットの値が 0x0015〜0x0020 の範囲内の場合、フレームはサブ署名と整合します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] pattern 1 offset 8 mask ffff 15 to 20

2.1.115 permit-channel

Syntax

permit-channel *channel-id-list*

undo permit-channel { *channel-id-list* | **all** }

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

channel-id-list: 許可された 10 個までのチャネルアイテムの空間分離リストを指定します。各アイテムは、*value1* **to** *value2* の形式でチャネル番号もしくはチャネル番号の範囲を指定します。チャネル番号の範囲は 1～224 です。*value2* 引数の値は *value1* 引数の値以上でなければなりません。

all: 許可されたすべてのチャネルを指定します。

説明

permit-channel コマンドは許可されたチャネルリストに 1 つあるいは複数のチャネルを追加します。

undo permit-channel コマンドは許可されたチャネルリストから指定されたチャネルあるいはすべてのチャネルを削除します。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、このコマンドを使用して許可されたチャネルリストを設定します。

例

チャネル 1 を許可されたチャネルリストに追加します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] permit-channel 1

関連コマンド

prohibited-channel

2.1.116 power-save

Syntax

power-save [**interval** *interval-value* | **minoffpacket** *packet-value* | **onoffpercent** *percent-value* | **quiet** *quiet-value*] *

undo power-save

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

interval *interval-value*: パワーセーブフレームのための統計値収集間隔を指定します。*interval-value* 引数の値は 1～3600 秒です。デフォルト値は 10 秒です。

minoffpacket *packet-value*: パワーセーブ攻撃分析を引き起こすパワーセーブ off フレームの数のしきい値を指定します。クライアントからの off フレームの数がしきい値の達すると、WIPS はパワーセーブ攻撃が発生したかどうか判断するために、パワーセーブフレームを分析します。値の範囲は 10～150 です。デフォルト値は 50 です。

onoffpercent *percent-value*: クライアントからのパワーセーブ on フレームと off フレームの比率のしきい値を指定します。しきい値に達すると WIPS はパワーセーブ攻撃のアラームを引き起こします。値の範囲は 0～100 です。デフォルト値は 80 です。

quiet *quiet-value*: WIPS がパワーセーブ攻撃のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内にパワーセーブ攻撃を検出してもアラームを引き起こしません。

説明

power-save コマンドはパワーセーブ攻撃検出を有効にします。

undo power-save コマンドはパワーセーブ攻撃検出を無効にします。

例

パワーセーブ攻撃検出を有効にします。*interval-value*、*packet-value*、*percent-value*、*quiet-value* の値をそれぞれ、20、20、90、100 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] power-save interval 20 minoffpacket 20 onoffpercent 90 quiet 100

2.1.117 prohibited-channel

Syntax

prohibited-channel [**quiet** *quiet-value*]

undo prohibited-channel

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が禁止されたチャネルのアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 です。デフォルトは 600 秒です。WIPS は遅延時間内に禁止されたチャネルを検出してもアラームを引き起こしません。

説明

prohibited-channel コマンドは禁止されたチャネル検出を有効にします。

undo prohibited-channel コマンドは禁止されたチャネル検出を無効にします。

WIPS がすべてのチャネルを禁止されたチャネルとして扱うことを防ぐため、禁止されたチャネル検出を設定する前に、**permit-channel** コマンドを使用して許可されたチャネルリストを設定します。

例

禁止されたチャネル検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] prohibited-channel quiet 100

関連コマンド

permit-channel

2.1.118 random-mac-scan

Syntax

random-mac-scan enable

undo random-mac-scan enable

デフォルト

WIPS は、ランダムな MAC アドレスを使用する Apple 端末のアラームをトリガーします。

View

Attack detection policy view

定義済みユーザロール

network-admin

説明

random-mac-scan enable コマンドはランダムな MAC アドレスを使用する Apple 端末のアラームをトリガーしないように WIPS を設定します。

undo random-mac-scan enable コマンドはデフォルトに戻します。

例

ランダムな MAC アドレスを使用する Apple 端末のアラームをトリガーしないように WIPS を設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] random-mac-scan enable

2.1.119 report-interval

Syntax

report-interval *interval*

undo report-interval

デフォルト

AP は、検出されたデバイスに関する情報を 30000 ミリ秒ごとに報告します。

View

User view

定義済みユーザロール

network-admin

パラメータ

interval: 検出されたデバイスに関する情報を AP がレポートする間隔を 1000~300000 ミリ秒の範囲で指定します。

説明

report-interval コマンドは検出されたデバイスに関する情報を AP が報告する間隔を設定します。

undo report-interval コマンドはデフォルトに戻します。

例

検出されたデバイスに関する情報を AP が報告する間隔を 10000 ミリ秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] report-interval 10000

2.1.120 reset wips embedded-oui

Syntax

reset wips embedded-oui

View

User view

定義済みユーザロール

network-admin

説明

report-interval コマンドは、OUI ライブラリ内のすべての埋め込み OUI を削除します。

例

OUI ライブラリの埋め込み OUI をすべて削除します。

<AP> reset wips embedded-oui

関連コマンド

- **export oui**
- **import oui**

2.1.121 reset wips statistics

Syntax

reset wips statistics

View

User view

定義済みユーザロール

network-admin

説明

reset wips statistics コマンドはすべてのセンサから収集した情報を消去します。

例

すべてのセンサから収集した情報を消去します。

<AP> reset wips statistics

関連コマンド

display wips statistics receive

2.1.122 reset wips virtual-security-domain

Syntax

reset wips virtual-security-domain *vsd-name* **device** { **ap** { **all** | **mac-address** *mac-address* } | **client** { **all** | **mac-address** *mac-address* } | **all** }

View

User view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

device: 装置のエントリを消去します。

ap: AP のエントリを消去します。

all: すべての AP のエントリを消去します。

mac-address *mac-address*: AP のエントリを消去します。*mac-address* 引数は AP の MAC アドレスをあらわします。

client: クライアントのエントリを消去します。

all: すべてのクライアントのエントリを消去します。

mac-address *mac-address*: クライアントのエントリを消去します。*mac-address* 引数はクライアントの MAC アドレスをあらわします。

all: すべての AP とクライアントのエントリを消去します。

説明

reset wips virtual-security-domain コマンドは VSD にある学習した AP もしくはクライアントのエントリを消去します。

例

VSD **aaa** にある学習した AP とクライアントのエントリを消去します。

<AP> reset wips virtual-security-domain aaa device all

関連コマンド

display wips virtual-security-domain device

2.1.123 reset wips virtual-security-domain countermeasure record

Syntax

reset wips virtual-security-domain *vsd-name* **countermeasure record**

View

User view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

reset wips virtual-security-domain countermeasure record コマンドは WIPS が不正な装置に対して講じた対策に関する情報を消去します。

例

VSD **aaa** のために WIPS が不正な装置に対して講じた対策に関する情報を消去します。

<AP> reset wips virtual-security-domain aaa countermeasure record

関連コマンド

display wips virtual-security-domain countermeasure record

2.1.124 rssi-change-threshold

Syntax

rssi-change-threshold *threshold-value*

undo rssi-change-threshold

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

threshold-value: ワイヤレス装置検出の RSSI 差分しきい値を 1~100 の範囲で指定します。。

説明

rssi-change-threshold コマンドは AP の RSSI と整合するように AP 分類ルールを設定します。

undo rssi-change-threshold コマンドはデフォルトに戻します。

例

ワイヤレス装置検出の RSSI 差分しきい値を 80 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] rssi-change-threshold 80

2.1.125 rssi-threshold

Syntax

rssi-threshold { **ap** *ap-rssi-value* | **client** *client-rssi-value* }

undo rssi-threshold { **ap** | **client** }

デフォルト

設定なし

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

ap *ap-rssi-value* :AP の RSSI しきい値を 1~100 の範囲で指定します。

client *client-rssi-value*: クライアントの RSSI しきい値を 1~100 の範囲で指定します。

説明

rssi-threshold コマンドはクライアントまたは AP の RSSI しきい値を設定します。

undo rssi-threshold コマンドはデフォルトに戻します。

例

AP の RSSI しきい値を 80 に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] rssi-threshold ap 80

2.1.126 rssi

Syntax

rssi *value1* [**to** *value2*]

undo rssi

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 [**to** *value2*]: AP の RSSI の値の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～100 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

rssi コマンドは AP の RSSI と整合するように AP 分類ルールを設定します。

undo rssi コマンドはデフォルトに戻します。

例

AP が 20～40 の RSSI と整合するように AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] rssi 20 to 40

2.1.127 security

Syntax

security { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }

undo security

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

equal: 指定されたセキュリティモードと等しいセキュリティモードと整合します。

include: 指定されたセキュリティモードを含むセキュリティモードと整合します。

clear: 消去するセキュリティモードを指定します。

wep: WEP セキュリティモードを指定します。

wpa: WPA セキュリティモードを指定します。

wpa2: WPA2 セキュリティモードを指定します。

説明

security コマンドは AP に使用されるセキュリティモードと整合するように AP 分類ルールを設定します。

undo security コマンドはデフォルトに戻します。

例

WEP セキュリティモードを使用する AP と整合するように AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] security equal wep

2.1.128 select sensor all

Syntax

select sensor all

undo select sensor all

デフォルト

直近で攻撃者を検出したセンサのみ、その攻撃者に対して対策を講じます。

View

Countermeasure policy view

定義済みユーザロール

network-admin

説明

select sensor all コマンドは攻撃者を検出するすべてのセンサを有効にします。

undo select sensor all コマンドは設定を削除します。

例

攻撃者に対して対策を講じるために、攻撃者を検出するすべてのセンサを有効にします。

<AP> system-view

[AP] wips

[AP-wips] countermeasure policy home

[AP-wips-ctm-home] select sensor all

2.1.129 seq-number

Syntax

seq-number *seq-value1* [**to** *seq-value2*]

undo seq-number

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

seq-value1 [**to** *seq-value2*]: フレームのシーケンス番号の範囲を指定します。*seq-value1* 引数と *seq-value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*seq-value 1* 引数と *seq-value 2* 引数の値の範囲は、どちらも 0～4095 です。ただし、*seq-value 2* 引数の値は *seq-value 1* 引数の値より大きくなければなりません。

説明

seq-number コマンドはシーケンス番号をもつフレームと整合するサブ署名を設定します。

undo seq-number コマンドはデフォルトに戻します。

例

シーケンス番号 100 をもつフレームと整合するサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] seq-number 100

2.1.130 signature policy

Syntax

signature policy *policy-name*

undo signature policy *policy-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

policy-name: 署名ポリシー名を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

signature policy コマンドは署名ポリシーを作成し、その view に移行します。指定された署名ポリシーがすでに存在する場合、signature policy view に移行します。

undo signature policy コマンドは署名ポリシーを削除します。

例

署名ポリシー**home** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] signature policy home

2.1.131 signature rule

Syntax

signature rule *rule-id*

undo signature rule *rule-id*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

rule-id: 署名の ID を指定します。範囲は 1～65535 です。

説明

signature rule コマンドは署名を作成し、その view に移行します。指定された署名がすでに存在する場合、signature view に移行します。

undo signature rule コマンドは署名を削除します。

例

signature 1 を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

2.1.132 soft-ap

Syntax

soft-ap [**convert-time** *time-value*]

undo soft-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

convert-time *time-value*: ソフト AP がクライアントと AP の役割を切り替える間隔を指定します。*time-value* 引数の値の範囲は 5〜600 秒です。デフォルト値は 10 秒です。

説明

soft-ap コマンドはソフト AP 検出を有効にします。

undo soft-ap コマンドはソフト AP 検出を無効にします。

例

ソフト AP 検出を有効にします。*time-value* 引数の値を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] soft-ap convert-time 100

2.1.133 ssid (AP classification rule view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*

undo ssid

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

ssid-string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドは AP に対して無線装置の SSID を整合するように AP 分類ルールを設定します。

undo ssid コマンドはデフォルトに戻します。

例

SSID **abc** の無線サービスを使用した AP を整合するために AP classification rule 1 を設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] ssid equal abc

2.1.134 ssid (signature view)

Syntax

ssid [**case-sensitive**] [**not**] { **equal** | **include** } *string*

undo ssid

デフォルト

設定なし

View

Signature view

定義済みユーザロール

network-admin

パラメータ

case-sensitive: SSID の大文字、小文字を区別します。

not: 指定された SSID と一致しない SSID、もしくは指定された SSID を含まない SSID を整合します。

equal: 指定された SSID と一致する SSID を整合します。

include: 指定された SSID を含む SSID を整合します。

string: SSID を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

説明

ssid コマンドはフレームの SSID を整合するためにサブ署名を設定します。

undo ssid コマンドはデフォルトに戻します。

例

signature 1 に対して SSID **office** のフレームを整合するためにサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-rule-1] ssid equal office

2.1.135 ssid-length

Syntax

ssid-length *length-value1* [**to** *length-value2*]

undo ssid-length

デフォルト

設定なし

View

Signature rule

定義済みユーザロール

network-admin

パラメータ

length-value1 [**to** *length-value2*]: SSID 長の値の範囲を指定します。*length-value1* 引数と *length-value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*length-value 1* 引数と *length-value 2* 引数の値の範囲は、どちらも 1～32 です。ただし、*length-value 2* 引数の値は *length-value 1* 引数の値より大きくなければなりません。

説明

ssid-length コマンドはフレームの SSID 長を整合するためにサブ署名を設定します。

undo ssid-length コマンドはデフォルトに戻します。

例

SSID 長が 10 のフレームを整合するためにサブ署名を設定します。

<AP> system-view

[AP] wips

[AP-wips] signature rule 1

[AP-wips-sig-1] ssid-length 10

2.1.136 trust mac-address

Syntax

trust mac-address *mac-address*

undo trust mac-address { *mac-address* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

mac-address: MAC アドレスを指定します。

all: すべての MAC アドレスを指定します。

説明

trust mac-address コマンドは許可された装置リストに AP もしくはクライアントの MAC アドレスを追加します。

undo trust mac-address コマンドは許可された装置リストから 1 つあるいはすべての MAC アドレスを削除します。

例

許可された装置リストに MAC アドレス **78AC-C0AF-944F** を追加します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] trust mac-address 78AC-C0AF-944F

2.1.137 trust oui

Syntax

trust oui *oui*

undo trust oui { *oui* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

oui: OUI の名前を指定します。大文字と小文字を区別しません。文字数は 6 文字です。

all: すべての OUI を指定します。

説明

trust oui コマンドは信頼された OUI リストに OUI を追加します。

undo trust oui コマンドは信頼された OUI リストから 1 つあるいはすべての OUI を削除します。

例

信頼された OUI リストに OUI **000fe4** と **000fe5** を追加します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] trust oui 000fe4

[AP-wips-cls-home] trust oui 000fe5

2.1.138 trust ssid

Syntax

trust ssid *ssid-name*

undo trust ssid { *ssid-name* | **all** }

デフォルト

設定なし

View

Classification policy view

定義済みユーザロール

network-admin

パラメータ

ssid-name: SSID の名前を指定します。大文字と小文字を区別します。文字数は 1～32 文字です。

all: すべての SSID を指定します。

説明

trust ssid コマンドは信頼された SSID リストに SSID を追加します。

undo trust ssid コマンドは信頼された SSID リストから 1 つあるいはすべての SSID を削除します。

例

信頼された SSID リストに SSID **flood1** を追加します。

<AP> system-view

[AP] wips

[AP-wips] classification policy home

[AP-wips-cls-home] trust ssid flood1

2.1.139 unencrypted-authorized-ap

Syntax

unencrypted-authorized-ap [**quiet** *quiet-value*]

undo unencrypted-authorized-ap

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可 AP を検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可 AP を検出してもアラームを引き起こしません。

説明

unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を有効にします。

undo unencrypted-authorized-ap コマンドは暗号化されていない許可 AP 検出を無効にします。

例

暗号化されていない許可 AP 検出を有効にします。遅延時間を 10 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] unencrypted-authorized-ap quiet 10

2.1.140 unencrypted-trust-client

Syntax

unencrypted-trust-client [**quiet** *quiet-value*]

undo unencrypted-trust-client

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が暗号化されていない許可クライアントを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5～604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に暗号化されていない許可クライアントを検出してもアラームを引き起こしません。

説明

unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を有効にします。

undo unencrypted-trust-client コマンドは暗号化されていない許可クライアント検出を無効にします。

例

暗号化されていない許可クライアント検出を有効にします。遅延時間を 10 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] unencrypted-trust-client quiet 10

2.1.141 up-duration

Syntax

up-duration *value1* [**to** *value2*]

undo up-duration

デフォルト

設定なし

View

AP classification rule view

定義済みユーザロール

network-admin

パラメータ

value1 [**to** *value2*]: AP の動作時間の値の範囲を指定します。*value1* 引数と *value2* 引数は、それぞれ値の範囲の始めと終わりを指定します。*value1* 引数と *value2* 引数の値の範囲は、どちらも 0～2592000 です。ただし、*value2* 引数の値は *value1* 引数の値より大きくなければなりません。

説明

up-duration コマンドを使用して、AP の動作時間と整合するように AP 分類ルールを設定します。

undo up-duration コマンドでデフォルトに戻します。

例

2000～40000 秒の動作時間の AP と整合するように AP 分類ルールを設定します。

<AP> system-view

[AP] wips

[AP-wips] ap-classification rule 1

[AP-wips-cls-rule-1] up-duration 2000 to 40000

2.1.142 virtual-security-domain

Syntax

virtual-security-domain *vsd-name*

undo virtual-security-domain *vsd-name*

デフォルト

設定なし

View

WIPS view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

virtual-security-domain コマンドは VSD を作成し、その view に移行します。

undo virtual-security-domain コマンドは VSD を削除します。

例

VSD **office** を作成し、その view に移行します。

<AP> system-view

[AP] wips

[AP-wips] virtual-security-domain office

[AP-wips-vsd-office]

2.1.143 weak-iv

Syntax

weak-iv [**quiet** *quiet-value*]

undo weak-iv

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS がウィーク IV のアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内にウィーク IV を検出してもアラームを引き起こしません。

説明

weak-iv コマンドはウィーク IV 検出を有効にします。

undo weak-iv コマンドはデフォルトに戻します。

例

ウィーク IV 検出を有効にします。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] weak-iv

2.1.144 windows-bridge

Syntax

windows-bridge [**quiet** *quiet-value*]

undo windows-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が Windows ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に Windows ブリッジを検出してもアラームを引き起こしません。

説明

windows-bridge コマンドは Windows ブリッジ検出を有効にします。

undo wireless-bridge コマンドは Windows ブリッジを無効にします。

例

Windows ブリッジ検出を有効にします。遅延時間を 360 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] windows-bridge quiet 360

2.1.145 wips(system view)

Syntax

wips

undo wips

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

説明

wips コマンドは WIPS view に移行します。

undo wips コマンドは WIPS view 内の設定をすべて削除します。

例

WIPS view に移行します。

<AP> system-view

[AP] wips

[AP-wips]

2.1.146 wips(radio view)

Syntax

wips { disable | enable }

undo wips

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: WIPS を無効にします。

enable: WIPS を有効にします。

説明

wips enable コマンドは WIPS を有効にし、Radio を WISP センサにします。

wips disable コマンドは WIPS を無効にします。

undo wips コマンドはデフォルトに戻します。

無線通信と WIPS センサは同じ Radio 上での併用をサポートしています。

無線通信と WIPS センサを併用している Radio の WIPS スキャンは、通信への影響を与えないために、端末との通信のないタイミングで行われます。

また、無線通信と WIPS センサが有効な Radio に対する通信、および端末の接続に対しては、通信を優先するため WIPS 検出はできません。

例

WLAN-radio 1/0/1 の WIPS を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-wlan-radio-1] wips enable

2.1.147 wips virtual-security-domain

Syntax

wips virtual-security-domain *vsd-name*

undo wips virtual-security-domain

デフォルト

AP view では、AP は AP group view で設定を使用します。

AP group view では、AP グループは VSD に追加されません。

View

AP view

定義済みユーザロール

network-admin

パラメータ

vsd-name: VSD の名前を指定します。大文字と小文字を区別します。文字数は 1～63 文字です。

説明

wips virtual-security-domain コマンドは AP を VSD に追加します。

undo wips virtual-security-domain コマンドは AP を VSD から削除します。

例

AP group **apgroup1** を VSD **office** に追加します。

<AP> system-view

[AP] wlan ap-group apgroup1

[AP-wlan-ap-group-apgroup1] wips virtual-security-domain office

2.1.148 wireless-bridge

Syntax

wireless-bridge [**quiet** *quiet-value*]

undo wireless-bridge

デフォルト

無効

View

Attack detection policy view

定義済みユーザロール

network-admin

パラメータ

quiet *quiet-value*: WIPS が無線ブリッジを検出してアラームを引き起こした後に、遅延時間を指定します。*quiet-value* 引数の値の範囲は 5〜604800 秒です。デフォルトは 600 秒です。WIPS は遅延時間内に無線ブリッジを検出してもアラームを引き起こしません。

説明

wireless-bridge コマンドは無線ブリッジ検出を有効にします。

undo wireless-bridge コマンドは無線ブリッジを無効にします。

例

無線ブリッジ検出を有効にします。遅延時間を 100 秒に設定します。

<AP> system-view

[AP] wips

[AP-wips] detect policy home

[AP-wips-dtc-home] wireless-bridge quiet 100

QX-W610 アクセスポイント

コマンドマニュアル

09.WLAN ローミング

本マニュアルは以下に示す章で構成されています。

01-WLAN ローミング

目次

このセクションのページは **9-x-x** です。

1 章 WLAN ローミング 1-1
1.1 WLAN ローミング設定コマンド 1-1
1.1.1 client cache aging-time 1-1
1.1.2 display wlan mobility roam-track mac-address 1-3
1.2 WLAN 802.11r ローミングコマンド 1-4
1.2.1 ft enable 1-4
1.2.2 ft method 1-5
1.2.3 ft reassociation-timeout 1-6
1.3 モビリティグループコマンド 1-7
1.3.1 authentication-mode 1-7
1.3.2 display wlan mobility 1-8
1.3.3 display wlan mobility group 1-10
1.3.4 group enable 1-11
1.3.5 member 1-12
1.3.6 snmp-agent trap enable wlan mobility 1-13
1.3.7 source 1-14
1.3.8 tunnel-type 1-15
1.3.9 wlan mobility group 1-16
1.3.10 wlan mobility-group-isolation enable 1-17
1.4 WLAN 802.11v コマンド 1-18
1.4.1 bss transition-management disassociation 1-18
1.4.2 bss transition-management enable 1-19
1.4.3 sacp anti-sticky 1-20

1章 WLAN ローミング

1.1 WLANローミング設定コマンド

1.1.1 client cache aging-time

Syntax

client cache aging-time aging-time

undo client cache aging-time

デフォルト

180 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

aging-time: エージングタイムを指定します。設定範囲は 0～86400 秒です。エージングタイムを 0 に設定した場合、クライアントがオフラインになった直後にクライアントのキャッシュ情報を削除します。

説明

client cache aging-time コマンドはクライアントキャッシュエージングタイムを設定します。

undo client cache aging-time コマンドはデフォルトに戻します。

このコマンドを実行する前に、サービステンプレートが無効であることを確認してください。

クライアントキャッシュは、クライアント用の PMK リストやアクセス VLAN などの情報を保存します。キャッシュエージングタイムが経過する前に、クライアントが別の AP にローミングすると、キャッシュ情報は継承されます。キャッシュエージングタイムが経過してもクライアントがオンラインにならない場合、そのキャッシュ情報は消去されます。

例

エージングタイムを 100 秒に設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] client cache aging-time 100

1.1.2 display wlan mobility roam-track mac-address

Syntax

display wlan mobility roam-track mac-address *mac-address*

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac-address *mac-address*: クライアントの MAC アドレスを指定します。

説明

display wlan mobility roam-track mac-address コマンドはホーム AP 上のクライアントのローミング情報を表示します。最新のローミングトラック情報が最初に表示されます。

例

#ホーム AP 上の指定されたクライアントのローミング情報を表示します。

<AP> display wlan mobility roam-track mac-address 5250-0012-0411

```
Total entries: 2
BSSID         Created at          Online time      AP IP address  RID  AP name
3ce5-a68d-2280  2017-03-14 11:12:28  00hr 48min 46sec  192.168.0.2    2    ap1
3ce5-a608-1150  2017-03-14 11:12:05  00hr 40min 46sec  127.0.0.1      2    ap2
```

表 1-1 コマンド出力

フィールド	説明
BSSID	クライアントが関連付けられているAPのBSSIDです。
Created at	クライアントのローミングトラックエントリが作成された日時。
Online time	クライアントのオンライン時間。
AP IP address	モビリティグループに使用される認証方式です。
RID	クライアントが関連付けられている無線のIDです。
AP name	クライアントが関連付けられているAPの名前です。

1.2 WLAN 802.11r ローミングコマンド

1.2.1 ft enable

Syntax

ft enable

undo ft enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

ft enable コマンドは FT（Fast BSS Transition）を有効にします。

undo ft enable コマンドは FT を無効にします。

FT により、クライアントが BSS から同一 ESS の別の BSS にローミングする際の遅延が短縮されます。802.11r FT を使用すると、クライアントはローミング先の AP とメッセージを交換する必要があります。FT は 2 つのメッセージ交換方法を提供します。

FT を有効にする場合、サービステンプレートが無効であることを確認してください。

FT を有効にするサービステンプレートは、security-ie rsn、client association-location ac を使用し、WPA3 と enhanced-open が無効である必要があります。

例

FT を有効にします。

<AP> system-view

[AP] wlan service-template st

[AP-wlan-st-st] ft enable

関連コマンド

security-ie

1.2.2 ft method

Syntax

ft method { **over-the-air** | **over-the-ds** }

undo ft method

デフォルト

over-the-air

View

Service template view

定義済みユーザロール

network-admin

パラメータ

over-the-air: Over-the-air FT を指定します。この方法では、クライアントは事前ローミング認証のためにローミング先の AP と直接通信できます。

over-the-DS: Over-the-DS FT を指定します。この方法では、クライアントは事前ローミング認証のために現在接続している AP を経由してローミング先の AP と通信します。

説明

ft method コマンドは FT 方法を設定します。

undo ft method コマンドはデフォルトに戻します。

FT 方法を設定する場合、サービステンプレートが無効であることを確認してください。

このコマンドは FT が有効の場合にのみ適用されます。

例

FT 方法を Over-the-DS に設定します。

<AP> system-view

[AP] wlan service-template st

[AP-wlan-st-st] ft method over-the-ds

関連コマンド

ft enable

1.2.3 ft reassociation-timeout

Syntax

ft reassociation-timeout *timeout*

undo ft reassociation-timeout

デフォルト

20 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

timeout: 再関連付けタイムアウトタイマを 1～100 秒の範囲で指定します。

説明

ft reassociation-timeout コマンドは再関連付けタイムアウトタイマを設定します。

undo ft reassociation-timeout コマンドはデフォルトに戻します。

再関連付けタイムアウトタイマを設定する場合、サービステンプレートが無効であることを確認してください。

このコマンドは FT が有効の場合のみ適用されます。

タイムアウトタイマが終了する前にクライアントが再関連付け要求を送信しない場合、ローミングプロセスは終了されます。

例

再関連付けタイムアウトタイマを 30 秒に設定します。

<AP> system-view

[AP] wlan service-template st

[AP-wlan-st-st] ft reassociation-timeout 30

関連コマンド

ft enable

1.3 モビリティグループコマンド

1.3.1 authentication-mode

Syntax

authentication-mode *authentication-mode* **[cipher | simple]** *authentication-key*

undo authentication-mode

デフォルト

IADTP 制御メッセージの認証モードは設定されていません。AP は IADTP 制御メッセージの完全性を検証しません。

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

authentication-mode: 認証モードを指定します。128 ビット MD 5 認証モードのみサポートします。

cipher: 暗号テキストの認証キーを指定します。

simple: プレーンテキストの認証キーを指定します。

authentication-key: 認証キーの文字列を設定します。大文字と小文字を区別します。**simple** を指定した場合、プレーンテキストで 1～16 の文字列でなくてはなりません。**cipher** を設定した場合、33～53 文字の暗号テキストでなければなりません。セキュリティのため、プレーンテキストのキーを含むすべてのキーは暗号化されて保存されます。

説明

authentication-mode コマンドは IADTP 制御メッセージの認証モードを設定します。

undo authentication-mode コマンドはデフォルトに戻します。

例

#モビリティグループ aaa の 認証モードを MD5 に設定し、認証キー12345 をプレーンテキストで設定します。

<AP> system-view

[AP] wlan mobility group aaa

[AP] authentication-mode md5 simple 12345

1.3.2 display wlan mobility

Syntax

display wlan mobility { roam-in | roam-out } [member ip *ipv4-address* **]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

roam-in: 別の AP からローミングしたクライアントに関する情報を表示します。

roam-out: 別の AP にローミングしたクライアントに関する情報を表示します。

member ip *ipv4-address*: メンバ AP の IPv4 アドレスを指定します。

説明

display wlan mobility コマンドは AP 間でローミングしたクライアントに関する情報を表示します。

例

AP にローミングしたすべてのクライアントに関する情報を表示します。

<AP> display wlan mobility roam-in

```
Total entries: 1
MAC address    BSSID         VLAN ID  HA IP address
5250-0012-0411  cbab-abab-abab  1       192.168.0.101
```

指定されたメンバ AP にローミングしたクライアントに関する情報を表示します。

<AP> display wlan mobility roam-in member ip 192.168.0.101

```
Total entries: 1
MAC address    BSSID         VLAN ID
5250-0012-0411  cbab-abab-abab  1
```

#別の AP にローミングしたすべてのクライアントに関する情報を表示します。

<AP> display wlan mobility roam-out

```
Total entries: 1
MAC address    BSSID         VLAN ID  Online time      FA IP address
5250-0012-0411  cbab-abab-abab  1       00hr 01min 39sec  192.168.0.102
```

#指定されたメンバ AP から別の AP にローミングしたクライアントに関する情報を表示します。

[AP] display wlan mobility roam-out member ip 192.168.0.102

```
Total entries: 1
MAC address    BSSID         VLAN ID  Online time
5250-0012-0411  cbab-abab-abab  1       00hr 03min 02sec
```

表 1-2 コマンド出力

フィールド	説明
MAC address	クライアントのMACアドレス
BSSID	クライアントが関連付けられているAPのBSSID
VLAN ID	クライアントのVLAN ID
Online time	クライアントのオンライン時間
HA IP address	クライアントのローミング元APのIPアドレス
FA IP address	クライアントのローミング先APのIPアドレス

1.3.3 display wlan mobility group

Syntax

display wlan mobility group [member ip *ipv4-address* **]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

member ip *ipv4-address*: メンバ AP の IPv4 アドレスを指定します。

このキーワードを指定しない場合、コマンドはモビリティ グループ情報を表示します。

説明

display wlan mobility group コマンドはモビリティグループ情報を表示します。

例

モビリティグループ情報を表示します。

<AP> display wlan mobility group

```
Mobility group name: office
 Tunnel type: IPv4
 Source IPv4: 172.16.220.101
 Source IPv6: Not configured
 Authentication method: Not configured
 Mobility group status: Enabled
 Member entries: 2
 IP address                      State        Online time
 172.16.220.102                   Down         00hr 00min 00sec
 172.16.220.105                   Up           00hr 36min 27sec
```

表 1-3 コマンド出力

フィールド	説明
Tunnel type	モビリティグループのIADTPトンネルタイプです。 • IPv4 • IPv6
Source IPv4	IADTPトンネルの確立に使用する送信元IPv4アドレスです。

フィールド	説明
Source IPv6	IADTPトンネルの確立に使用する送信元IPv6アドレスです。
Authentication method	モビリティグループに使用される認証方式です。
Mobility group status	モビリティグループのステータスです。 ● enable ● disable
IP address	メンバAPのIPアドレスです。
State	IADTPトンネルのステータスです。 ● UP ● DOWN
Online time	メンバAPのオンライン時間です。

モビリティ グループのメンバ デバイスに関する情報を表示します。

<Sysname> display wlan mobility group member ip 172.16.220.105

```
IP address : 172.16.220.105
State : UP
Interface : WLAN-Tunnel0
Online duration : 00hr 36min 35sec
```

表 1-4 コマンド出力

フィールド	説明
IP address	メンバーデバイスのIPアドレス
State	IADTP tunnel ステート: ・UP. ・DOWN.
Interface	IADTP tunnelのインターフェイスのタイプと番号
Online duration	メンバーデバイスのオンライン期間

関連コマンド

wlan mobility group

1.3.4 group enable

Syntax

group enable

undo group enable

デフォルト

無効

View

Mobility group view

定義済みユーザロール

network-admin

説明

group enable コマンドはモビリティグループを有効にします。

undo group enable コマンドはモビリティグループを無効にします。

例

#モビリティグループ floor 1 を有効にします。

<AP> system-view

[AP] wlan mobility group floor1

[AP-wlan-mg-floor1] tunnel-type ipv4

[AP-wlan-mg-floor1] source ip 192.168.0.1

[AP-wlan-mg-floor1] member ip 192.168.0.2

[AP-wlan-mg-floor1] group enable

関連コマンド

- **member**
- **source**
- **tunnel-type**
- **wlan mobility group**

1.3.5 member

Syntax

member ip *ip-address* [**vlan** *vlan-id-list*]

undo member [**ip** *ip-address*] [**vlan** [*vlan-id-list*]]

デフォルト

メンバ AP の設定なし

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: メンバ AP の IPv4 アドレスを指定します。

vlan *vlan-id-list*: 最大 10 個の VLAN アイテムのスペース区切りリストを指定します。

各項目は、VLAN ID または VLAN ID の範囲を vlan-id1 から vlan-id2 の形式で指定します。VLAN ID の値の範囲は 2 ～ 4094 です。vlan-id2 引数の値は、vlan-id1 引数の値より小さくすることはできません。

説明

member コマンドはモビリティグループメンバを追加します。

undo member コマンドはモビリティグループメンバを削除します。

モビリティグループが無効の場合のみ、メンバの追加・削除が可能です。モビリティグループのメンバは、IADTP トンネルの確立に使用される IP アドレスによって識別されます。AP は 1 つのモビリティグループだけに属することが出来ます。モビリティグループには、最大 31 のモビリティグループメンバを追加できます。**undo member** コマンドの使用時に、IP アドレスを省略した場合、モビリティグループ内のすべてのメンバを削除します。

例

モビリティグループメンバ を追加します。

<AP> system-view

[AP] wlan mobility group abc

[AP-wlan-mg-abc] member ip 192.168.1.55 vlan 3 10 19 22 to 30

1.3.6 snmp-agent trap enable wlan mobility

Syntax

snmp-agent trap enable wlan mobility

undo snmp-agent trap enable wlan mobility

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap enable wlan mobility コマンドは、WLAN ローミングの SNMP 通知を有効にします。

undo snmp-agent trap enable wlan mobility コマンドは、WLAN ローミングの SNMP 通知を無効にします。

重要な WLAN ローミング イベントを NMS に報告するには、WLAN ローミングの SNMP 通知を有効にします。

WLAN ローミング イベント通知が正しく送信されるようにするには、デバイスで SNMP を設定する必要があります。

例

WLAN ローミングの SNMP 通知を有効にします。

<AP> system-view

[AP] snmp-agent trap enable wlan mobility

1.3.7 source

Syntax

source ip *ipv4-address*

undo source [ip]

デフォルト

送信元 IP アドレスの設定なし。

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ip *ipv4-address*: 送信元 IPv4 アドレスを指定します。

説明

source コマンドは、IADTP トンネルを確立するための送信元 IP アドレスを指定します。

undo source コマンドは、IADTP トンネルを確立するための送信元 IP アドレスを削除します。

デバイスは、送信元 IP アドレスを使用して、メンバ AP との IADTP トンネルを確立します。IADTP トンネルを確立するために送信元 IP アドレスを指定する場合は、次の制限とガイドラインに従ってください。

- モビリティグループが無効になっていることを確認してください。
- IPv4 アドレスを指定できますが、IADTP トンネルの IP アドレスタイプと同じ IP アドレスタイプのみが有効になります。

undo コマンドを使用するときに IP アドレスを指定しない場合、このコマンドはすべての送信元 IP アドレスを削除します。

例

IADTP トンネルを確立するための送信元 IPv4 アドレス 192.168.1.55 を設定します。

<AP> system-view

[AP] wlan mobility group abc

[AP-wlan-mg-abc] source ip 192.168.1.55

関連コマンド

- **group enable**
- **member**

1.3.8 tunnel-type

Syntax

tunnel-type ipv4

undo tunnel-type

デフォルト

IPv4

View

Mobility group view

定義済みユーザロール

network-admin

パラメータ

ipv4: トンネルタイプを IPv4 アドレスタイプに指定します。

説明

tunnel-type コマンドは、IADTP トンネルの IP アドレス タイプを指定します。

undo tunnel-type コマンドはデフォルトに戻します。

このコマンドを実行する前に、モビリティ グループが無効になっていることを確認してください。

例

モビリティ グループ aaa の IADTP トンネルの IP アドレスタイプを IPv4 に設定します。

<AP> system-view

[AP] wlan mobility group aaa

[AP-wlan-mg-aaa] tunnel-type ipv4

1.3.9 wlan mobility group

Syntax

wlan mobility group *group-name*

undo wlan mobility group *group-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name: モビリティグループ名を指定します。名前は、大文字と小文字を区別せず、スペースを含まない 1 ～ 15 文字の文字列です。

説明

wlan mobility group コマンドはモビリティグループを作成し、そのビューに移行するか、既存のモビリティグループのビューに移行します。

undo wlan mobility group を使用してデフォルトに戻します。

メンバ AP に設定するモビリティグループ名は、同じ名前である必要があります。

1 つの AP に作成できるモビリティグループは 1 つだけです。

例

#モビリティグループ office を作成し、その View に移行します。

<AP> system-view

[AP] wlan mobility group office

[AP-wlan-mg-office]

1.3.10 wlan mobility-group-isolation enable

Syntax

wlan mobility-group-isolation enable

undo wlan mobility-group-isolation enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

wlan mobility-group-isolation enable を使用して、モビリティグループのトンネル分離を有効にします。

undo wlan mobility-group-isolation enable コマンドは、モビリティグループのトンネル分離を無効にします。

このコマンドは、モビリティグループ内の AP 間にループが存在する場合に必要です。このコマンドにより、AP はモビリティグループ内のトンネル間でパケットを転送できなくなり、ブロードキャストストームが回避されます。

例

モビリティグループのトンネル分離を有効にします。

<AP> system-view

[AP] wlan mobility-group-isolation enable

1.4 WLAN 802.11vコマンド

1.4.1 bss transition-management disassociation

Syntax

bss transition-management disassociation { **forced** | **recommended** } [**timer** *time*]

undo bss transition-management disassociation

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

パラメータ

forced: アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はそのクライアントを強制的にログオフします。

recommended: アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はクライアントを強制的にログオフしません。

time: アソシエーション解除タイマを 0～180 秒の範囲で指定します。デフォルトのタイマは 90 秒です。このタイマを 0 に設定すると、bss transition-management disassociation forced が有効の場合、AP は BTM 要求をクライアントに送信した直後に、そのクライアントを強制的にログオフします。bss transition-management disassociation recommended が有効の場合、AP はクライアントに BTM 要求を送信した後、そのクライアントからログオフしません。

説明

bss transition-management disassociation コマンドは BTM アソシエーション解除を設定します。

undo bss transition-management disassociation コマンドはデフォルトに戻します。

BTM のアソシエーション解除を有効にするには、まず BTM を有効にします。BTM アソシエーション解除を設定する場合、サービステンプレートが無効であることを確認してください。

BTM アソシエーション解除が設定されている場合、AP はクライアントから BTM query ーを受信すると BTM request をクライアントに送信し、BSS 移行のためにクライアントを案内します。

bss transition-management disassociation forced を設定すると、アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合に、クライアントが強制的にログオフされます。この機能は慎重に使用してください。

例

BTM のアソシエーション解除(forced)を有効にし、タイマを 60 秒に設定します

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] bss transition-management disassociation forced timer 60

関連コマンド

bss transition-management enable

sacp anti-sticky

1.4.2 bss transition-management enable

Syntax

bss transition-management enable

undo bss transition-management enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

bss transition-management enable コマンドは BTM を有効にします。

undo bss transition-management enable コマンドはデフォルトに戻します。

BTM を使用すると、接続中の AP の信号強度が低い場合や、より優れた AP が検出された場合に、クライアントは最適な AP にローミングできます。

client anti-sticky が無効の場合、AP はクライアントの信号強度がしきい値よりも低いかどうかを調べず、unsolicited BTM をトリガしません。

この作業を行う前に、サービステンプレートが無効になっていることを確認してください。

例

BTM を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] bss transition-management enable

関連コマンド

bss transition-management forced-disassociation

sacp anti-sticky

1.4.3 sacp anti-sticky

Syntax

sacp anti-sticky { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] [**forced-logoff**] }

undo sacp anti-sticky

デフォルト

有効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

rssi *rssi-value*: RSSI しきい値を 5～100(dbm)の範囲で設定します。デフォルトのしきい値は 20dbm です。

interval *interval*: 検出間隔を 3～10(秒)の範囲で設定します。デフォルトの検出間隔は 3 秒です。

forced-logoff: 信号強度がRSSIしきい値よりも低い非802.11vクライアントをログオフします。

説明

sacp anti-sticky enable コマンドはクライアント anti-sticky を有効にします。

sacp anti-sticky disable コマンドはクライアント anti-sticky を無効にします。

undo sacp anti-sticky コマンドはデフォルトに戻します。

この機能により、AP は指定された間隔でクライアントの信号強度を調べることができます。802.11v クライアントの場合、クライアントの信号強度が RSSI しきい値より低いと、関連付けられた AP が BSS 移行をトリガして、クライアントをより適切な BSS に導きます。802.11v 以外のクライアントの場合、アクションは実行されません。

例

AP1 の radio1 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします

<AC> system-view

[AC] wlan ap ap1 model QX-W1240

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1] sacp anti-sticky enable rssi 30 interval 5 forced-logoff

AP グループ 1 のモデル QX-W1240 の radio2 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします

<AC> system-view

[AC] wlan ap-group 1

[AC-wlan-ap-group-1] ap-model QX-W1240

[AC-wlan-ap-group-1-model-QX-W1240] radio 2

[AC-wlan-ap-group-1-model-QX-W1240-radio-2] sacp anti-sticky enable rssi 30 interval 5 forced-logoff

関連コマンド

bss transition-management disassociation

bss transition-management enable

QX-W610 アクセスポイント

コマンドマニュアル

10. WLAN トラフィック

本マニュアルは以下に示す章で構成されています。

01-ユーザアイソレーション

目次

このセクションのページは **10-x-x** です。

1 章 ユーザアイソレーション 1-1
1.1 ユーザアイソレーション設定コマンド 1-1
1.1.1 display user-isolation statistics 1-1
1.1.2 reset user-isolation statistics 1-3
1.1.3 user-isolation enable 1-4
1.1.4 user-isolation permit-broadcast 1-5
1.1.5 user-isolation vlan enable 1-6
1.1.6 user-isolation vlan permit-mac 1-7

1章 ユーザアイソレーション

1.1 ユーザアイソレーション設定コマンド

1.1.1 display user-isolation statistics

Syntax

display user-isolation statistics [**vlan** *vlan-id*]

Views

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

vlan *vlan-id*: VLAN を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のユーザアイソレーションの統計情報を表示します。

説明

display user-isolation statistics コマンドは VLAN、あるいはすべての VLAN のユーザアイソレーションの統計情報を表示します。

例

すべての VLAN のユーザアイソレーションの統計情報を表示します。

<AP> display user-isolation statistics

```
Number of VLANs enabled with user isolation: 2
Number of VLANs disabled with user isolation: 1

VLAN     State       Drops         Permit unicast    Permitted MAC list
4        Enabled     0             Y                 N/A
6        Disabled    0             N                 0023-89a2-3d4d
                                                     0033-89a2-3d4a
5        Enabled     0             Y                 N/A
```

表 1-1 コマンド出力

フィールド	説明
VLAN	VLAN IDです。
State	VLANのユーザアイソレーションの状態です。 ● **Enabled**－有効です。 ● **Disabled**－無効です。
Drops	VLANで廃棄したパケット数です。
Permit unicast	VLANのユーザ間でユニキャストパケットが許可されるかどうかを示します。 ● **Y**－許可します。ブロードキャスト、マルチキャストパケットのみ隔離されます。 ● **N**－許可しません。ユニキャスト、ブロードキャスト、マルチキャストパケットのすべてのパケットが隔離されます。
Permitted MAC list	VLANの許可されているMACアドレスリストです。

関連コマンド

- **user-isolation vlan enable**
- **user-isolation vlan permit-mac**

1.1.2 reset user-isolation statistics

Syntax

reset user-isolation statistics [**vlan** *vlan-id*]

View

User view

定義済みユーザロール

network-admin

パラメータ

vlan *vlan-id*: VLAN を指定します。設定範囲は 1～4094 です。指定しない場合、すべての VLAN のユーザアイソレーションの統計情報を削除します。

説明

reset user-isolation statistics コマンドは VLAN、あるいはすべての VLAN のユーザアイソレーションの統計情報を削除します。

例

VLAN 1 のユーザアイソレーションの統計情報を削除します。

<AP> reset user-isolation statistics vlan 1

関連コマンド

- **user-isolation vlan enable**
- **user-isolation vlan permit-mac**

1.1.3 user-isolation enable

Syntax

user-isolation enable

undo user-isolation enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

user-isolation enable コマンドはユーザアイソレーションを有効にします。

undo user-isolation enable コマンドはデフォルトに戻します。

例

ユーザアイソレーションを有効にします。

<AP> system-view

[AP] wlan service-template 1

[AP -wlan-st-1] user-isolation enable

1.1.4 user-isolation permit-broadcast

Syntax

user-isolation permit-broadcast

undo user-isolation permit-broadcast

デフォルト

ユーザアイソレーションが有効な VLAN において、装置は有線のユーザから無線のユーザに送信されたブロードキャストトラフィック、あるいはマルチキャストトラフィックを転送しません。

View

System view

定義済みユーザロール

network-admin

説明

user-isolation permit-broadcast コマンドは有線のユーザから無線のユーザに送信されたブロードキャストトラフィックとマルチキャストトラフィックを許可します。

undo user-isolation permit-broadcast コマンドはデフォルトに戻します。

有線のユーザと無線のユーザが同一の VLAN に属しているときのみ、無線のユーザから有線のユーザへのブロードキャストパケットとマルチキャストパケットを隔離します。

例

有線のユーザから無線のユーザに送信されたブロードキャストトラフィックとマルチキャストトラフィックを許可します。

<AP> system-view

[AP] user-isolation permit-broadcast

関連コマンド

user-isolation vlan enable

1.1.5 user-isolation vlan enable

Syntax

user-isolation vlan *vlan-list* **enable** [**permit-unicast**]

undo user-isolation vlan *vlan-list* **enable**

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-id-list: VLAN を指定します。半角スペースで区切ることで 10 の VLAN を指定することができます。各 VLAN は VLAN ID で VLAN を指定あるいは *vlan-id1* **to** *vlan-id2* の形式で指定します。VLAN ID の設定範囲は 1～4094 です。VLAN の範囲を指定する場合、*vlan-id2* は *vlan-id1* よりも大きい値にしてください。

permit-unicast: ユーザ間のユニキャストパケットを許可します。指定しない場合、ブロードキャストパケット、マルチキャストパケットと同様にユニキャストパケットをユーザ間で隔離します。

説明

user-isolation vlan enable コマンドは VLAN リストのユーザアイソレーションを有効にします。

undo user-isolation vlan enable コマンドは VLAN リストのユーザアイソレーションを無効にします。

外部ネットワークへの切断を防ぐため、ゲートウェイの MAC アドレスを許可された MAC アドレスリストに割り当てます。許可された MAC アドレスを追加する場合、**user-isolation vlan permit-mac** コマンドを使用します。

user-isolation vlan enable コマンドを複数実行した場合、装置は指定された VLAN を累積します。

user-isolation vlan enable コマンドを VLAN 内で複数実行した場合、最後に行った設定を適用します。

例

VLAN 1 のユーザアイソレーションを有効にします。

<AP> system-view

[AP] user-isolation vlan 1 enable

1.1.6 user-isolation vlan permit-mac

Syntax

user-isolation vlan *vlan-list* **permit-mac** *mac-list*

undo user-isolation vlan *vlan-list* **permit-mac** { *mac-list* | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

vlan-list: VLAN を指定します。半角スペースで区切ることで 10 の VLAN を指定することができます。各 VLAN は VLAN ID で VLAN を指定あるいは *vlan-id1* **to** *vlan-id2* の形式で指定します。VLAN ID の設定範囲は 1～4094 です。VLAN の範囲を指定する場合、*vlan-id2* は *vlan-id1* よりも大きい値にしてください。

mac-list: MAC アドレスを指定します。半角スペースで区切ることで 16 の MAC アドレスを指定することができます。MAC アドレスの形式は H-H-H で指定します。ブロードキャスト MAC アドレス、マルチキャスト MAC アドレスを指定することはできません。

all: 許可されたすべての MAC アドレスを指定します。

説明

user-isolation vlan permit-mac コマンドは VLAN リストで許可された MAC アドレスリストを設定します。

undo user-isolation vlan enable コマンドは VLAN の許可された MAC アドレスリストを削除します。

許可された MAC アドレスをもつユーザからのパケットは対応する VLAN で隔離されません。

user-isolation vlan permit-mac コマンドは最大 16 の MAC アドレスを登録できます。

ソフトウェアバージョン 7.2.13 を含む以降のバージョンでは、最大 64 の MAC アドレスを登録できます。

例

VLAN 1 で MAC アドレス 00bb-ccdd-eeff、0022-3344-5566 を許可するように設定します。

<AP> system-view

[AP] user-isolation vlan 1 permit-mac 00bb-ccdd-eeff 0022-3344-5566

関連コマンド

- **display user-isolation statistics**
- **user-isolation vlan enable**

QX-W610 アクセスポイント

コマンドマニュアル

11. WLAN 拡張機能

本マニュアルは以下に示す章で構成されています。

01- WLAN 最適化

02- WLAN メッシュの設定

03-WLAN の高可用性の設定

目次

このセクションのページは **11-x-x** です。

1 章 WLAN 最適化 1-1
1.1 WLAN 最適化設定コマンド 1-1
1.1.1 option client fast-forwarding 1-1
1.1.2 option client hide-node-protection 1-2
1.1.3 option client reconnect 1-3
1.1.4 option keep active 1-4

1章 WLAN 最適化

1.1 WLAN最適化設定コマンド

1.1.1 option client fast-forwarding

Syntax

option client fast-forwarding enable level *level-value*

undo option client fast-forwarding

デフォルト

AP からクライアントへのデータフレームの高速転送モードは、3

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

level *level-value*: fast forwarding level を 1～4 の範囲で指定します。

説明

option client fast-forwarding enable コマンドは、AP からクライアントへのデータフレームの高速転送を有効にします。

undo option client fast-forwarding コマンドは、AP からクライアントへのデータフレームの高速転送を無効にします。

この機能により、AP は追加の処理 (検証やカウントなど) を行わずにデータフレームをクライアントに転送できるようになり、処理効率が向上します。

例

AP からクライアントへのデータフレームの高速転送（3）を有効にします。

<AP> system-view

[AP]interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] option client fast-forwarding enable level 3

1.1.2 option client hide-node-protection

Syntax

option client hide-node-protection enable

undo option client hide-node-protection

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

説明

option client hide-node-protection enable コマンドは隠れ端末保護を有効にします。

undo option client hide-node-protection コマンドはデフォルトに戻します。

このコマンドは、802.11g、802.11n、802.11ac クライアントにのみ有効です。

この機能を有効にすると、クライアントは隠れ端末からの干渉を避けるために RTS/CTS フレームを送信します。

本機能によって複数端末の通信衝突を軽減させることが可能です。

例

#Radio**1** に対して隠れ端末保護を有効にします。

<AP> system-view

[AP] interface WLAN-Radio1/0/1

[AP-WLAN-Radio1/0/1] option client hide-node-protection enable

1.1.3 option client reconnect

Syntax

option client reconnect enable [**rssi** *rssi-value*] [**interval** *interval*] }

undo option client reconnect

デフォルト

Radio view：AP group view の設定を使用します。

AP group radio view：無効

View

Radio view

AP group の radio view

定義済みユーザロール

network-admin

パラメータ

rssi *rssi-value*: RSSI しきい値を 5～100 の範囲で指定します。RSSI しきい値のデフォルト値および推奨値は、それぞれ 10 と 20 です。

interval *interval*: AP がクライアントの信号強度を検出する間隔を 3～10 秒の範囲で指定します。デフォルト設定は 3 秒です。

説明

option client reconnect コマンドは AP トリガのクライアント再関連付けを有効にします。

undo option client reconnect コマンドはデフォルトに戻します。

この機能により、クライアントの信号強度が指定した RSSI しきい値よりも小さいと AP が検知したとき、AP は再認証フレームをクライアントに送信できます。再認証フレームを受信したクライアントは、AP に再関連付け、あるいは別の AP にローミングできます。

例

Radio1 で RSSI しきい値を 30、検出間隔を 5 秒に設定します。

<AC> system-view

[AP] interface WLAN-Radio1/0/1

[AP-WLAN-Radio1/0/1] option client reconnect enable rssi 30 interval 5

1.1.4 option keep active

Syntax

option keep-active { disable | enable }

undo option keep-active

デフォルト

無効。

View

Radio interface view

定義済みユーザロール

network-admin

説明

option keep-active enable コマンドは無線クライアントのスリープ時間を短縮する機能を有効にします。

option keep-active disable コマンドは、無線クライアントのスリープ時間を短縮する機能を無効にします。

undo option keep-active コマンドはデフォルトに戻します。

スリープ状態の無線クライアントは、ビーコンフレーム内の TIM（トラフィック通知メッセージ）情報を定期的にリスニングすることで、接続している AP が無線クライアントのパケットをバッファしているかどうかを判断します。AP が無線クライアントのパケットをバッファしている場合、スリープ状態は終了し、AP とデータ通信を行います。本機能を有効にすると、AP はビーコンフレーム内の TIM を変更し、端末のスリープ時間を短縮して、伝送効率を向上させます。

例

Radio1 で無線クライアントのスリープ時間短縮機能を有効にします。

<AP> system-view

[AP] interface WLAN-Radio1/0/1

[AP-WLAN-Radio1/0/1] option keep-active enable

目次

このセクションのページは **11-x-x** です。

2 章 WLAN メッシュの設定 2-1
2.1 WLAN メッシュコマンド 2-1
2.1.1 akm mode sae 2-1
2.1.2 display wlan mesh-link 2-2
2.1.3 display wlan mesh-policy 2-3
2.1.4 display wlan mesh-profile 2-5
2.1.5 interface wlan-mesh 2-6
2.1.6 link-hold-rssi 2-7
2.1.7 link-initiation enable 2-8
2.1.8 link-keepalive 2-8
2.1.9 link-maximum-number 2-10
2.1.10 mesh-id 2-11
2.1.11 mesh-interface 2-11
2.1.12 mesh peer-mac-address 2-12
2.1.13 mesh-policy 2-13
2.1.14 mesh-profile 2-14
2.1.15 mesh-profile enable 2-15
2.1.16 preshared-key 2-16
2.1.17 probe-request-interval 2-17
2.1.18 wlan mesh-policy 2-18
2.1.19 wlan mesh-profile 2-19

2章 WLAN メッシュの設定

2.1 WLAN メッシュコマンド

2.1.1 akm mode sae

Syntax

akm mode sae

undo akm mode

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

説明

akm mode sae コマンドは akm（authentication and key management）モードを SAE（simultaneous authentication of equals）に設定します。

undo akm mode コマンドはデフォルトに戻します。

akm モードを設定する、あるいは削除する前に、メッシュプロファイルが無効であることを確認してください。

例

メッシュプロファイル 1 の akm モードを SAE に設定します。

<AP> system-view

[AP] wlan mesh-profile 1

[AP-wlan-mesh-profile-1] akm mode sae

関連コマンド

display wlan mesh-profile

2.1.2 display wlan mesh-link

Syntax

display wlan mesh-link [**mesh-profile** *mesh-profile-number* | **interface** *interface-type interface-number* | **peer-mac-address** *mac-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mesh-profile *mesh-profile-number*: メッシュプロファイルのプロファイル番号を指定します。値の範囲は 1～32 です。

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。

peer-mac-address *mac-address*: H-H-H 形式でピア MP の MAC アドレスを指定します。

説明

display wlan mesh-link コマンドはメッシュリンク情報を表示します。

パラメータを指定しない場合、すべてのメッシュリンクの情報を表示します。

例

全てのメッシュリンクの情報を表示します。

<AP> display wlan mesh-link

```
Peer MAC      RSSI BSSID         Interface       Link state Online time
 7b2d-23bb-e56f 22   4a1b-517d-23ff WLAN-MeshLink1   Active    00h 08m 31s
 6a3b-cc5a-e215 22   4a1b-517d-23ff WLAN-MeshLink2   Active    00h 40m 56s
```

表 2-1 コマンド出力

フィールド	説明
Peer MAC	ピアMPのMACアドレス
Interface	WLANメッシュリンクのインタフェース
Link state	リンク状態： ● Active－アクティブリンク メッシュリンクがアクティブです。 ● Active(T)－アクティブテンポラリリンク 一時的なメッシュリンク(テンポラリリンク)がアクティブです。テンポラリリンクは、初期状態で孤立しているFIT APとのみ一時的に確立されるメッシュリンクです。
Online time	メッシュリンクがアクティブな状態での経過時間

2.1.3 display wlan mesh-policy

Syntax

display wlan mesh-policy [*mesh-policy-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mesh-policy-name: 大文字と小文字を区別しない 1～31 文字でメッシュポリシーの名前を指定します。ポリシー名を指定しない場合、すべてのメッシュポリシーの情報を表示します。

説明

display wlan mesh-policy コマンドはメッシュポリシー情報を表示します。

例

全てのメッシュポリシーの情報を表示します。

<AP> display wlan mesh-policy

```
Mesh policy name          : default_mesh_policy
Mesh link initiation       : Enabled
Max links                 : 2
Probe request interval     : 1000 ms
Link hold RSSI            : 15 dBm
Link rate mode            : fixed

Mesh policy name          : abc
Mesh link initiation       : Enabled
Max links                 : 2
Probe request interval     : 1000 ms
Link hold RSSI            : 15 dBm
Link rate mode            : fixed

Mesh policy name          : bb
Mesh link initiation       : Enabled
Max links                 : 2
Probe request interval     : 1000 ms
Link hold RSSI            : 15 dBm
Link rate mode            : Fixed
```

表 2-2 コマンド出力

フィールド	説明
Mesh link initiation	メッシュリンク開始機能の状況： ● 有効 ● 無効

フィールド	説明
Max links	リンクの最大数
Link rate mode	リンクレートモード： ● Fixed－リンクは固定レートで動作しています。 ● Real-time－リンクレートはリアルタイムでRSSIに適応しています。

2.1.4 display wlan mesh-profile

Syntax

display wlan mesh-profile [*mesh-profile-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mesh-profile-number: メッシュプロファイルの番号を指定します。値の範囲は 1～32 です。メッシュプロファイルを指定しない場合、すべてのメッシュプロファイルの情報を表示します。

説明

display wlan mesh-profile コマンドはメッシュプロファイル情報を表示します。

例

全てのメッシュプロファイルの情報を表示します。

<AP> display wlan mesh-profile

```
Mesh profile number         : 1
Mesh ID                   : 11
Link keepalive interval     : 2 s
Mesh profile status         : Enabled
AKM mode                  : None
PSK status                : Disabled

Mesh profile number         : 2
Mesh ID                   : 22
Link keepalive interval     : 2 s
```

```
Mesh profile status         : Enabled
AKM mode                   : None
PSK status                  : Disabled
```

表 2-3 コマンド出力

フィールド	説明
Mesh profile status	メッシュプロファイルの状況： ● 有効 ● 無効
AKM mode	akmモード ● None－akmモードは指定されていません。 ● SAE－SAEモードが指定されています。
PSK status	事前共有鍵設定状況： ● Enabled－事前共有鍵が設定されています。 ● Disabled－事前共有鍵は設定されていません。

2.1.5 interface wlan-mesh

Syntax

interface wlan-mesh *interface-number*

undo interface wlan-mesh *interface-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: メッシュインタフェースの番号を指定します。値の範囲は 0～1023 です。

説明

interface wlan-mesh コマンドはメッシュインタフェースを作成し、その view に移行します。あるいは既存のメッシュインタフェースの view に移行します。

undo interface wlan-mesh コマンドはメッシュインタフェースを削除します。

例

メッシュインタフェース 3 を作成し、その view に移行します。

<AP> system-view

[AP] interface wlan-mesh 3

[AP-wlan-mesh3]

関連コマンド

mesh-interface

2.1.6 link-hold-rssi

Syntax

link-hold-rssi *value*

undo link-hold-rssi

デフォルト

15 dBm

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

value: メッシュリンクホールド RSSI を指定します。値の範囲は 5～100dBm です。

説明

link-hold-rssi コマンドはメッシュリンクホールド RSSI（メッシュリンクを保持するための最小信号強度）を設定します。

undo link-hold-rssi コマンドはデフォルトに戻します。

例

メッシュリンク **abc** に対してメッシュリンクホールド RSSI を 24dBm に設定します。

<AP> system-view

[AP] wlan mesh-policy abc

[AP-wlan-mesh-policy-abc] link-hold-rssi 24

関連コマンド

display wlan mesh-policy

2.1.7 link-initiation enable

Syntax

link-initiation enable

undo link-initiation enable

デフォルト

有効

View

Mesh policy view

定義済みユーザロール

network-admin

説明

link-initiation enable コマンドはメッシュリンク開始を有効にします。

undo link-initiation enable コマンドはメッシュリンク開始を無効にします。

メッシュリンク開始を有効にすることで、MP はリンクオープン要求を送信していないピアに対してリンクオープン要求を送信します。この機能が無効の場合、MP はピアがリンクオープン要求を送信するまで、ピアに対してリンクオープン要求を送信しません。

例

メッシュリンク開始を無効にします。

<AP> system-view

[AP] wlan mesh-policy abc

[AP-wlan-mesh-policy-abc] undo link-initiation enable

関連コマンド

display wlan mesh-policy

2.1.8 link-keepalive

Syntax

link-keepalive *keepalive-interval*

undo link-keepalive

デフォルト

2 秒

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

keepalive-interval: keepalive 間隔を指定します。値の範囲は 1～1800 秒です。

説明

link-keepalive コマンドはメッシュリンク keepalive 間隔を設定します。

undo link-keepalive コマンドはデフォルトに戻します。

メッシュリンクの MP はメッシュリンク状態を検出するために keepalive パケットを使用します。大きい MAC アドレスをもつ MP は、keepalive 間隔で keepalive パケットをピアの端に送信します。keepalive パケットを送信した MP は、連続して 3 回の keepalive 間隔終了前に応答を受信しない場合、メッシュリンクを切断します。また、keepalive パケットを受信した MP は、連続して 3 回の keepalive 間隔終了前に keepalive パケットを受信しない場合、メッシュリンクを切断します。リンク状態を正しく検出するため、送信側の keepalive 間隔は、受信側の keepalive 間隔の 3 倍以下に設定してください。

例

メッシュプロファイル 1 でメッシュリンク keepalive 間隔を 6 秒に設定します。

<AP> system-view

[AP] wlan mesh-profile 1

[AP-wlan-mesh-profile-1] link-keepalive 6

関連コマンド

display wlan mesh-profile

2.1.9 link-maximum-number

> 🕮 **メモ：**
>
> ホップ数（ネットワーク内のメッシュリンクの最長経路）が増加するにつれてスループットは低下します。

Syntax

link-maximum-number *max-link-number*

undo link-maximum-number

デフォルト

2

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

max-link-number: メッシュリンクの最大数を指定します。値の範囲は 1～8 です。

説明

link-maximum-number コマンドはラジオのメッシュリンクの最大数を設定します。

undo link-maximum-number コマンドはデフォルトに戻します。

MP はメッシュリンクが最大数に達すると、ラジオでの新規メッシュリンクの確立を停止します。

例

メッシュポリシー**abc** に対してメッシュリンクの最大数を 5 に設定します。

<AP> system-view

[AP] wlan mesh-policy abc

[AP-wlan-mesh-policy-abc] link-maximum-number 5

関連コマンド

display wlan mesh-policy

2.1.10 mesh-id

Syntax

mesh-id *mesh-id*

undo mesh-id

デフォルト

設定なし

View

Mesh profile view

定義済みユーザロール

network-admin

パラメータ

mesh-id: メッシュ ID を指定します。大文字と小文字を区別する 1～32 文字で指定できます。

説明

mesh-id コマンドはメッシュプロファイルにメッシュ ID に割り当てます。

undo interface wlan-mesh コマンドはデフォルトに戻します。

例

メッシュプロファイル 1 にメッシュ ID を割り当てます。

<AP> system-view

[AP] wlan mesh-profile 1

[AP-wlan-mesh-profile-1] mesh-id mesh

関連コマンド

display wlan mesh-profile

2.1.11 mesh-interface

Syntax

mesh-interface *interface-number*

undo mesh-interface

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

interface-number: メッシュインタフェースの番号を指定します。値の範囲は 0～1023 です。

説明

mesh-interface コマンドはラジオにメッシュインタフェースをバインドします。

undo mesh-interface コマンドはデフォルトに戻します。

1 つのラジオに対して 1 つのメッシュインタフェースをバインドできます。このコマンドを複数回実行した場合、最後に実行したものが適用されます。

例

WLAN-Radio 1/0/1 にメッシュインタフェース 3 をバインドします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] mesh-interface 3

関連コマンド

interface wlan-mesh

2.1.12 mesh peer-mac-address

Syntax

mesh peer-mac-address [**blacklist**] *mac-address*

undo mesh peer-mac-address [**blacklist**] [*mac-address*]

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

blacklist: MP の MAC アドレスをメッシュピアブラックリストに追加します。このパラメータを指定しない場合、MAC アドレスはメッシュピアホワイトリストに追加されます。

mac-address: MP の MAC アドレスを H-H-H 形式で指定します。

説明

mesh peer-mac-address コマンドはメッシュピアブラックリストもしくはホワイトリストに MP を追加します。メッシュインタフェースを作成し、その view に移行します。あるいは既存のメッシュインタフェースの view に移行します。

undo mesh peer-mac-address コマンドはメッシュピアブラックリストもしくはホワイトリストから MP を削除します。

ブラックリストとホワイトリストの両方を設定した場合、ホワイトリストのみ適用されます。

同じ MAC アドレスをホワイトリストもしくはブラックリストに追加するために、このコマンドを複数回実行した場合、最後の設定が適用されます。

例

メッシュインタフェース 3 を作成し、その view に移行します。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] mesh peer-mac-address 4ab7-c78a-44ff

2.1.13 mesh-policy

Syntax

mesh-policy name *policy-name*

undo mesh-policy

デフォルト

デフォルトメッシュポリシーの **default_mesh_policy** がラジオにバインドされています。

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

policy-name: メッシュポリシー名を指定します。大文字と小文字を区別しない 1～31 文字で指定できます。

説明

mesh-policy コマンドはメッシュポリシーをラジオにバインドします。

undo mesh-policy コマンドはデフォルトに戻します。

1 つのラジオに 1 つのメッシュポリシーをバインドできます。このコマンドを複数回実行した場合、最後に実行したものが適用されます。

例

メッシュポリシー**policy3** を作成し、WLAN-Radio 1/0/2 にバインドします。

<AP> system-view

[AP] interface wlan-radio 1/0/2

[AP-WLAN-Radio1/0/2] mesh-policy name policy3

関連コマンド

mesh-profile enable

wlan mesh-profile

2.1.14 mesh-profile

Syntax

mesh-profile *mesh-profile-number*

undo mesh-profile

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

interface-number: メッシュインタフェースの番号を指定します。値の範囲は 0～1023 です。

説明

interface wlan-mesh コマンドはメッシュインタフェースを作成し、その view に移行します。あるいは既存のメッシュインタフェースの view に移行します。

undo interface wlan-mesh コマンドはメッシュインタフェースを削除します。

例

メッシュインタフェース 3 を作成し、その view に移行します。

<AP> system-view

[AP] interface wlan-mesh 3

[AP-wlan-mesh3]

関連コマンド

mesh-interface

2.1.15 mesh-profile enable

Syntax

mesh-profile enable

undo mesh-profile enable

デフォルト

無効

View

Mesh profile view

定義済みユーザロール

network-admin

説明

mesh-profile enable コマンドはメッシュプロファイルを有効にします。

undo mesh-profile enable コマンドはメッシュプロファイルを無効にします。

メッシュプロファイルを有効にする前に、メッシュ ID を割り当てる必要があります。

例

メッシュプロファイル 1 を有効にします。

<AP> system-view

[AP] wlan mesh-profile 1

[AP-wlan-mesh-profile-1] mesh-profile enable

関連コマンド

mesh-id

2.1.16 preshared-key

Syntax

preshared-key { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*

undo preshared-key

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

pass-phrase: 文字列形式で鍵を設定します。

raw-key: 16 進数形式で鍵を設定します。

cipher: 暗号化形式で鍵を指定します。

simple: 平文形式で鍵を指定します。安全のため、平文形式で指定された鍵は暗号化形式で格納されます。

string: 大文字と小文字を区別する鍵列を指定します。鍵の長さの範囲は以下の通りです。

- **pass-phrase plaintext**－8～63 文字
- **pass-phrase ciphertext**－41～117 文字
- **raw-key plaintext**－64 桁の 16 進数字
- **raw-key ciphertext**－117 文字

説明

preshared-key コマンドはメッシュプロファイルに事前共有鍵を追加します。

undo preshared-key コマンドはデフォルトに戻します。

このコマンドを使用する前に、メッシュプロファイルが無効であることを確認してください。

メッシュプロファイルに設定できる事前共有鍵は 1 つです。このコマンドを複数回実行した場合、最後の設定が適用されます。

例

メッシュプロファイル 1 に平文の事前共有鍵 **abcdefghij** を追加します。

<AP> system-view

[AP] wlan mesh-profile 1

[AP-wlan-mesh-profile-1] preshared-key pass-phrase simple abcdefghij

関連コマンド

display wlan mesh-profile

2.1.17 probe-request-interval

Syntax

probe-request-interval *interval-value*

undo probe-request-interval

デフォルト

1000 ミリ秒

View

Mesh policy view

定義済みユーザロール

network-admin

パラメータ

interval-value: 100～8191 ミリ秒の範囲で間隔を指定します。

説明

probe-request-interval コマンドはプローブ要求間隔を設定します。

undo probe-request-interval コマンドはデフォルトに戻します。

例

メッシュポリシーa**bc** に対してプローブ要求間隔を 500 ミリ秒に設定します。

<AP> system-view

[AP] wlan mesh-policy abc

[AP-wlan-mesh-policy-abc] probe-request-interval 500

関連コマンド

display wlan mesh-policy

2.1.18 wlan mesh-policy

Syntax

wlan mesh-policy *policy-name*

undo wlan mesh-policy *policy-name*

デフォルト

システム定義のポリシー「**default_mesh_policy**」が存在します。

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name：メッシュポリシーの名前を指定します。英数字と記号を入力することができます。入力可能な文字数は 1 から 31 文字です。

英文字は大文字と小文字を区別せずに入力することができます。

記号は、アンダースコア（_）、ハイフン（-）、大カッコ（[]）、スラッシュ（/）、ピリオド（.）を入力することができます。大文字と小文字を区別しない 1～31 文字で指定できます。

説明

wlan mesh-policy コマンドはメッシュポリシーを作成し、その view に移行します。あるいは既存のメッシュポリシーの view に移行します。

undo wlan mesh-policy コマンドはメッシュポリシーを削除します。

ラジオで使用中のメッシュポリシー内の属性設定を削除、修正する前に、ラジオにバインドされたメッシュプロファイルを無効にしてください。

システム定義のメッシュポリシーを修正もしくは削除することはできません。

例

メッシュポリシー**abc** を作成し、その view に移行します。

<AP> system-view

[AP] wlan mesh-policy abc

[AP-wlan-mesh-policy-abc]

関連コマンド

mesh-interface

2.1.19 wlan mesh-profile

Syntax

wlan mesh-profile *mesh-profile-number*

undo wlan mesh-profile *mesh-profile-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

mesh-profile-number: メッシュプロファイルの番号を指定します。値の範囲は 1～32 です。

説明

wlan mesh-profile コマンドはメッシュプロファイルを作成し、その view に移行します。あるいは既存のメッシュプロファイルの view に移行します。

undo wlan mesh-profile コマンドはメッシュプロファイルを削除します。

メッシュプロファイル内の属性設定を修正するには、メッシュプロファイルを無効にする必要があります。

例

メッシュプロファイル 1 を作成し、その view に移行します。

<AP> system-view

[AP] wlan mesh-profile 1

[AP-wlan-mesh-profile-1]

関連コマンド

mesh-profile enable

目次

このセクションのページは **11-x-x** です。

3 章 WLAN の高可用性の設定 3-1
3.1 WLAN アップリンク検出コマンド 3-1
3.1.1 wlan uplink track 3-1

3章 WLAN の高可用性の設定

3.1 WLANアップリンク検出コマンド

3.1.1 wlan uplink track

Syntax

wlan uplink track *track-entry-number*

undo wlan uplink track

デフォルト

WLAN アップリンク検出はトラックエントリと関連付けられていません。

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: トラックエントリ ID を指定します。範囲は 1～1024 です。

説明

wlan uplink track コマンドはWLANアップリンク検出をトラックエントリと関連付けます。

undo wlan uplink track コマンドはデフォルトに戻します。

本コマンドにより、トラックエントリに関連付けられたアップリンク状態に基づいて無線状態を AP が調節できるようになります。トラックエントリが Negative 状態の場合、AP はすべての無線を無効にします。トラックエントリが Positive 状態の場合、AP はすべての無線を有効にします。

本コマンドを複数回実行した場合、最新の設定が有効になります。

例

トラックエントリ 1 を WLAN アップリンク検出に関連付けます。

<AP> system-view

[AP] wlan uplink track 1

QX-W610 アクセスポイント

コマンドマニュアル

12. ユーザアクセスと認証

本マニュアルは以下に示す章で構成されています。

01-WLAN 認証

02-WLAN IP スヌーピング

03-AAA

04-802.1X

05-MAC アドレス認証

目次

このセクションのページは **12-x-x** です。

1 章 WLAN 認証 1-1
1.1 WLAN 認証設定コマンド 1-1
1.1.1 client-security authentication fail-vlan 1-1
1.1.2 client-security authentication-mode 1-2
1.1.3 client-security authorization-fail offline 1-4
1.1.4 client-security ignore-authorization 1-5
1.1.5 client-security intrusion-protection action 1-6
1.1.6 client-security intrusion-protection enable 1-7
1.1.7 client-security intrusion-protection timer temporary-block 1-8
1.1.8 client-security intrusion-protection timer temporary-service-stop 1-10
1.1.9 display wlan client-security block-mac 1-11
1.1.10 dot1x domain 1-12
1.1.11 dot1x handshake enable 1-13
1.1.12 dot1x handshake secure enable 1-14
1.1.13 dot1x max-user 1-15
1.1.14 dot1x re-authenticate enable 1-16
1.1.15 fail-permit enable 1-17
1.1.16 fail-permit template 1-18
1.1.17 mac-authentication domain 1-19
1.1.18 mac-authentication max-user 1-20

1章 WLAN 認証

1.1 WLAN認証設定コマンド

1.1.1 client-security authentication fail-vlan

Syntax

client-security authentication fail-vlan *vlan-id*

undo client-security authentication fail-vlan

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

vlan-id: WLAN 制限 VLAN の ID を指定します。範囲は 1〜4094 です。VLAN が作成されていることを確認してください。

説明

client-security authentication fail-vlan コマンドは、サービステンプレートで WLAN 制限 VLAN を設定します。

undo client-security authentication fail-vlan コマンドは、デフォルトにします。

組織のセキュリティ戦略を遵守しないことが原因で WLAN 認証に失敗したクライアントを、WLAN の制限 VLAN に収容することができます。例えば、間違ったパスワードやユーザ名を入力したクライアントに制限 VLAN が適用されます。制限 VLAN は認証タイムアウトあるいはネットワークの接続問題のために認証に失敗した WLAN クライアントに適用しません。

本コマンドは、サービステンプレートが無効なときに設定可能であり、サービステンプレートが有効になると適用されます。

例

サービステンプレート 1 で制限 VLAN として VLAN 10 を設定します。

<AP> system-view

[AP] wlan service-template 1

[AP-wlan-st-1] client-security authentication fail-vlan 10

1.1.2 client-security authentication-mode

Syntax

client-security authentication-mode { **dot1x** | **dot1x-then-mac** | **mac** | **mac-and-dot1x** | **mac-then-dot1x | oui-then-dot1x** }

undo client-security authentication-mode

デフォルト

設定なし。装置は認証を実行しません（認証バイパスモード）。クライアントは直接装置にアクセスすることができます。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot1x: 802.1X 認証のみを実行します。

dot1x-then-mac: 最初に 802.1X 認証を実行し、次に MAC アドレス認証を実行します。クライアントが 802.1X 認証を通過した場合は、MAC アドレス認証は実行されません。

mac: MAC アドレス認証のみを実行します。

mac-and-dot1x: MAC アドレス認証と 802.1X 認証の２つの認証（マルチステップ認証）を実行します。MAC アドレス認証を最初に実行し、MAC アドレス認証にパスした場合のみ、802.1X 認証を実行します。２つの認証にパスしたクライアントの接続が許可されます。

mac-then-dot1x: 最初に MAC アドレス認証を実行し、次に 802.1X 認証を実行します。クライアントが MAC 認証を通過した場合は、802.1X 認証は実行されません。

oui-then-dot1x: 最初に OUI 認証を実行し、次に 802.1X 認証を実行します。クライアントが OUI 認証を通過した場合は、802.1X 認証は実行されません。

説明

client-security authentication-mode コマンドは、WLAN クライアントの認証モードを設定します。

undo client-security authentication-mode コマンドは、デフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

サービステンプレートはどの認証モードにおいても複数の認証モードへのアクセスを許可します。802.1X クライアントの最大数を設定するには、**dot1x max-user** コマンドを使用します。MAC アドレス認証クライアントの最大数を設定するには、**mac-authentication max-user** コマンドを使用します。

例

サービステンプレート service1 でサービスにおける WLAN クライアントの認証モードを mac に設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] client-security authentication-mode mac

1.1.3 client-security authorization-fail offline

Syntax

client-security authorization-fail offline

undo client-security authorization-fail offline

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

client-security authorization-fail offline コマンドは、authentication-fail offline 機能を有効にします。

undo client-security authorization-fail offline コマンドは、デフォルトに戻します。

authorization-fail-offline 機能は ACL あるいはユーザプロファイルで許可されていない WLAN クライアントをログオフします。

以下の状況では、クライアントは ACL あるいはユーザプロファイルの許可に失敗します。

- 装置あるいはサーバは、クライアントに指定した ACL あるいはユーザプロファイルの許可に失敗する。
- 許可された ACL あるいはユーザプロファイルが存在しない。

本機能が無効の場合、装置は ACL あるいはユーザプロファイルの許可に失敗した WLAN クライアントをログオフしませんが、装置は失敗ログを残します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート service1 で authorization-fail-offline 機能を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] client-security authorization-fail offline

1.1.4 client-security ignore-authorization

Syntax

client-security ignore-authorization

undo client-security ignore-authorization

デフォルト

装置はサーバから受け取った認証情報を使用します。

View

Service template view

定義済みユーザロール

network-admin

説明

client-security ignore-authorization コマンドは装置が認証サーバ（RADIUS サーバやローカル装置）から受信した許可情報を無視するよう設定します。

undo client-security ignore-authorization コマンドはデフォルトに戻します。

このコマンドは、次のクライアントに適用されます。

- 802.1 X 認証を使用するクライアント。このコマンドを使用すると、装置は 802.1 X 認証の失敗を無視し、802.1 X 認証に失敗したクライアントをオンラインにすることができます。
- RADIUS ベースの MAC 認証とポータル認証の両方を使用するクライアント。
  通常、クライアントはネットワークリソースにアクセスするために、MAC 認証とポータル認証を渡す必要があります。クライアントは、ポータル認証が実行されるたびにユーザ名とパスワードを提供します。
  このコマンドは、クライアントの認証プロセスを次のように簡略化します。
  - RADIUS サーバがクライアントの MAC 認証情報をすでに記録している場合、クライアントは MAC 認証を渡します。装置を使用すると、クライアントはポータル認証を実行せずにネットワークリソースにアクセスできます。
  - RADIUS サーバがクライアントの MAC 認証情報を記録しない場合、クライアントは MAC 認証に失敗します。装置は MAC 認証の失敗を無視し、クライアントに対してポータル認証を実行します。クライアントがポータル認証に合格すると、クライアントはネットワークリソースにアクセスできます。ポータル認証クライアントの MAC アドレスは、MAC 認証情報として RADIUS サーバに記録されます。

このコマンドは、サービステンプレートが無効の場合に設定可能であり、サービステンプレートが有効になった後に有効になります。

RSN を使用して新しい AP にローミングする 802.1 X クライアントの場合は、このコマンドを使用しないでください。

例

サービステンプレート service1 で認証サーバからの許可情報を無視するよう設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] client-security ignore-authorization

1.1.5 client-security intrusion-protection action

Syntax

client-security intrusion-protection action { **service-stop** | **temporary-block** | **temporary-service-stop** }

undo client-security intrusion-protection action

デフォルト

temporary-block

View

Service template view

定義済みユーザロール

network-admin

パラメータ

service-stop: 無線インタフェースの BSS が手動で有効にされるまで、不正フレームが受信された BSS を停止します。

temporary-block: 一定期間、不正フレームの送信元 MAC アドレスをブロック MAC アドレスリストに追加します。期間の設定には **client-security intrusion-protection timer temporary-block** コマンドを使用します。

temporary-service-stop: 一定期間、不正フレームが受信された BSS を停止します。期間の設定には **intrusion-protection timer temporary-service-stop** コマンドを使用します。

説明

client-security authentication-mode コマンドは、不正フレームを検出した場合、装置が実施する侵入保護アクションを設定します。

undo client-security intrusion-protection action コマンドは、デフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

本コマンドを適用するには、**client-security intrusion-protection enable** コマンドを使用して侵入保護機能を有効にする必要があります。

例

サービステンプレート service1 で、侵入保護機能が不正フレームを検出した装置で BSS を停止するよう設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] client-security intrusion-protection enable

[AP-wlan-st-service1] client-security intrusion-protection action service-stop

関連コマンド

- **client-security intrusion-protection enable**
- **client-security intrusion-protection timer temporary-block**
- **client-security intrusion-protection timer temporary-service-stop**

1.1.6 client-security intrusion-protection enable

Syntax

client-security intrusion-protection enable

undo client-security intrusion-protection enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

client-security intrusion-protection enable コマンドは侵入保護機能を有効にします。

undo client-security intrusion-protection enable コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

装置が不正なクライアントからの接続要求を受信した場合、要求を受信した BSS で事前定義された保護アクションを実行します。WLAN 認証に失敗した場合、その MAC アドレスのクライアントは不正クライアントになります。保護アクションを設定するには、**client-security intrusion-protection action** コマンドを使用します。

例

サービステンプレート service1 で、侵入保護機能を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] client-security intrusion-protection enable

関連コマンド

client-security intrusion-protection action

1.1.7 client-security intrusion-protection timer temporary-block

Syntax

client-security intrusion-protection timer temporary-block *time*

undo client-security intrusion-protection timer temporary-block

デフォルト

180 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

time: MAC アドレスがブロックされる期間を指定します。範囲は 60～300 秒です。

説明

client-security intrusion-protection timer temporary-block コマンドは侵入保護によって MAC アドレスがブロックされる期間を設定します。

undo client-security intrusion-protection timer temporary-block コマンドはデフォルトに戻します。

本コマンドは侵入保護アクションが **temporary-block** の場合のみ有効です。

サービステンプレートを有効にした後にブロック期間を変更した場合、新しい設定は、その後に検出した不正パケットに対して適用されます。

例

サービステンプレート service1 で、不正 MAC アドレスのブロック期間を 120 秒に設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] client-security intrusion-protection enable

[AP-wlan-st-service1] client-security intrusion-protection action temporary-block

[AP-wlan-st-service1] client-security intrusion-protection timer temporary-block 120

関連コマンド

- **client-security intrusion-protection action**
- **client-security intrusion-protection enable**

1.1.8 client-security intrusion-protection timer temporary-service-stop

Syntax

client-security intrusion-protection timer temporary-service-stop *time*

undo client-security intrusion-protection timer temporary-service-stop

デフォルト

20 秒

View

Service template view

定義済みユーザロール

network-admin

パラメータ

time: BSS が停止する期間を指定します。範囲は 10～300 秒です。

説明

client-security intrusion-protection timer temporary-service-stop コマンドは侵入保護による BSS 停止期間を設定します。

undo client-security intrusion-protection timer temporary-service-stop コマンドはデフォルトに戻します。

本コマンドは侵入保護アクションが **temporary-service-stop** の場合のみ適用されます。

サービステンプレートを有効にした後に BSS 停止期間を変更した場合、新しい設定は、その後に検出した不正パケットに対して適用されます。

例

サービステンプレート service1 で、BSS 停止期間を 30 秒に設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] client-security intrusion-protection enable

[AP-wlan-st-service1] client-security intrusion-protection action temporary-service-stop

[AP-wlan-st-service1] client-security intrusion-protection timer temporary-service-stop 30

関連コマンド

- **client-security intrusion-protection action**
- **client-security intrusion-protection enable**

1.1.9 display wlan client-security block-mac

Syntax

display wlan client-security block-mac

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display wlan client-security block-macコマンドはWLANクライアントのブロックされた MAC アドレス情報を表示します。

侵入保護アクションが **temporary-block** である場合、認証に失敗した MAC アドレスがブロック MAC アドレスリストに追加されます。

例

すべてのブロックされた MAC アドレス情報を表示します。

<AP> display wlan client-security block-mac

```
MAC address        AP ID      RADIO ID    BSSID
0002-0002-0002     1          1           00ab-0de1-0001
000d-88f8-0577     1          1           0ef1-0001-02c1

Total entries: 2
```

表 1-1 コマンド出力

フィールド	説明
MAC address	ブロックされたMACアドレス。（H-H-H形式）
AP ID	ブロックされたMACアドレスのAP ID
RADIO ID	ブロックされたMACアドレスの無線ID
BSSID	ブロックされたMACアドレスのBSS-ID（H-H-H形式）
Total entries	ブロックされたMACアドレスの数

関連コマンド

- **client-security intrusion-protection action**
- **client-security intrusion-protection timer temporary-block**

1.1.10 dot1x domain

Syntax

dot1x domain *domain-name*

undo dot1x domain

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメイン名を指定します。設定範囲は 1～255 文字です。大文字小文字を区別ません。

説明

dot1x domain コマンドはサービステンプレートで 802.1X クライアントのための認証ドメインを指定します。

undo dot1x domain コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

802.1X は以下の順番で WLAN クライアントのための認証ドメインを選択します。

1) サービステンプレートで指定された認証ドメイン
2) ユーザ名で指定されたドメイン
3) デフォルト認証ドメイン

例

サービステンプレート service1 で、802.1X クライアントのための認証ドメインとして my-domain を指定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] dot1x domain my-domain

1.1.11 dot1x handshake enable

Syntax

dot1x handshake enable

undo dot1x handshake enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x handshake enable コマンドは 802.1X オンラインユーザハンドシェイク機能を有効にします。

undo dot1x handshake enable コマンドは 802.1X オンラインユーザハンドシェイク機能を無効にします。

オンラインユーザハンドシェイク機能は、定期的にクライアントにハンドシェイクメッセージを送信することにより、オンライン 802.1X クライアントの接続状態を確認します。最大ハンドシェイク試行回数に到達してもハンドシェイクタイマ内にクライアントから応答を受信しない場合、装置はクライアントをオフライン状態にします。ハンドシェイクタイマの設定には、**dot1x timer handshake-period** コマンドを使用します。最大ハンドシェイク試行回数の設定には、**dot1x retry** コマンドを使用します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

例

サービステンプレート service1 で、802.1X クライアントのためのオンラインユーザハンドシェイク機能を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] dot1x handshake enable

関連コマンド

- **dot1x handshake secure enable**
- **dot1x retry** （コマンドマニュアルのセクション 12 *ユーザアクセスと認証 “802.1X”*）

- **dot1x timer handshake-period**（コマンドマニュアルのセクション 12 *ユーザアクセスと認証　“802.1X”*）

1.1.12 dot1x handshake secure enable

Syntax

dot1x handshake secure enable

undo dot1x handshake secure enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x handshake secure enable コマンドは 802.1X オンラインユーザハンドシェイクセキュリティ機能を有効にします。

undo dot1x handshake secure enable コマンドは 802.1X オンラインユーザハンドシェイクセキュリティ機能を無効にします。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

オンラインユーザハンドシェイクセキュリティ機能を適用するには、オンラインユーザハンドシェイク機能が有効になっている必要があります。

オンラインユーザハンドシェイクセキュリティ機能は、認証されたオンラインの 802.1X クライアントのみを保護します。

例

サービステンプレート service1 で、802.1X クライアントのためのオンラインユーザハンドシェイクセキュリティ機能を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] dot1x handshake enable

[AP-wlan-st-service1] dot1x handshake secure enable

関連コマンド

dot1x handshake enable

1.1.13 dot1x max-user

Syntax

dot1x max-user *count*

undo dot1x max-user

デフォルト

512

View

Service template view

定義済みユーザロール

network-admin

パラメータ

count: 同時接続 802.1X クライアントの最大数を設定します。範囲は 1～512 です。

説明

dot1x　max-user コマンドはサービステンプレートで 802.1X クライアントの最大同時接続数を設定します。

undo dot1x max-user コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

最大数に達した場合、サービステンプレートは以降の 802.1X クライアントを拒否します。

🕮 **メモ：**

- 802.1X 認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は、QX-W610 では 128 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

例

サービステンプレート service1 で、802.1X クライアントの最大接続数を 100 に設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] dot1x max-user 100

1.1.14 dot1x re-authenticate enable

Syntax

dot1x re-authenticate enable

undo dot1x re-authenticate enable

デフォルト

無効

View

Service template view

定義済みユーザロール

network-admin

説明

dot1x re-authenticate enable コマンドは 802.1X クライアントの定期的なオンラインユーザ再認証機能を有効にします。

undo dot1x re-authenticate enable コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

定期的再認証により、サービステンプレートにおいてオンラインの 802.1X クライアントを装置が定期的に認証することが可能になります。本機能はオンラインクライアントの接続状態を確認し、サーバによって割り当てられた許可属性をアップデートします。属性には ACL、VLAN ベースのユーザプロファイルが含まれます。

dot1x timer reauth-period コマンドにより、再認証の間隔を設定することができます。

サーバによって割り当てられた RADIUS 属性の Session-Timeout、Termination-Action は、定期的なオンラインユーザの再認証に影響します。サーバによって割り当てられた Session-Timeout、Termination-Action を表示するには、**display dot1x connection** コマンドを使用します。（コマンドマニュアルのセクション 12 *ユーザアクセスと認証 “802.1X”* を参照してください）。

- Termination-Action が Default（ログオフ）の場合、テンプレート内のオンラインユーザ再認証は、定期的再認証タイマがセッションタイムアウトタイマよりも小さい場合のみ適用されます。
- Termination-Action が Radius-request の場合、テンプレート内のオンラインユーザ再認証は動作しません。装置は、セッションタイムアウトタイマの期限切れ後にオンライン 802.1X クライアントを再認証します。

例

サービステンプレート service1 で、802.1X クライアントの定期的再認証機能を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] dot1x re-authenticate enable

関連コマンド

dot1x timer（コマンドマニュアルのセクション 12 *ユーザアクセスと認証 “802.1X”*）

1.1.15 fail-permit enable

Syntax

fail-permit enable [**keep-online**]

undo fail-permit enable

デフォルト

無効

Views

Service template view

定義済みユーザロール

network-admin

パラメータ

keep-online: 失敗許可機能が動作する際、オンラインのクライアントが切断されるのを防ぎます。

説明

fail-permit enable コマンドは失敗許可機能を有効にします。

undo fail-permit enable コマンドは失敗許可機能を無効にします。

失敗許可機能は以下の目的で使用します。

- **認証失敗許可**—RADIUS サーバもしくは AC と AP が切断されたあと、802.1X 認証、MAC 認証、もしくは PSK 認証クライアントがネットワークにアクセスできるようになります。RADIUS サーバもしくは AC との切断が発生すると、AP はクライアントに対して継続してアクセスサービスを提供し、トラフィックを転送します。

fail-permit enable コマンドは、サービステンプレートが無効になっている場合にのみ実行でき、サービステンプレートが有効になった後に有効になります。

fail-permit enable コマンドと **fail-permit template** コマンドを同一のサービステンプレートに設定しないでください。

例

#サービステンプレートで失敗許可機能を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] fail-permit enable

関連コマンド

fail-permit template

1.1.16 fail-permit template

Syntax

fail-permit template

undo fail-permit template

デフォルト

設定なし

Views

Service template view

定義済みユーザロール

network-admin

説明

fail-permit template コマンドはレーダによる通信停止回避のため、もしくは 802.1X 認証での失敗許可機能のためのバックアップ用サービステンプレートとして指定します。

undo fail-permit template コマンドはレーダによる通信停止回避のため、もしくは 802.1X 認証での失敗許可機能のためのバックアップ用サービステンプレート指定を削除します。

レーダによる通信停止回避を行うためには 1 つのサービステンプレートに対して､1 つのバックアップ用のサービステンプレートを用意します。

- バックアップ用サービステンプレートには、fail-permit service template コマンドを追加する点を除き、オリジナルのサービステンプレートと同じ設定を含める必要があります。
- バックアップ用サービステンプレートは、オリジナルのサービステンプレートとは異なる無線にバインドする必要があります。

802.1X 認証で失敗許可機能を使用する場合、サービステンプレートを 2 つ設定します。1 つのサービステンプレートには 802.1X 認証の設定および **fail-permit enable** コマンドを設定します。もう一方のサービステンプレートにはバックアップ用に PSK 認証および **fail-permit template** コマンドを設定します。AP が RADIUS サーバと通信不能になるまではバックアップ用の SSID は表示されません｡AP が RADIUS サーバと通信不能になってから数分後に失敗許可機能が動作します。接続済みのクライアントは接続を維持します。新規クライアントは、失敗許可機能動作後に接続可能です。RADIUS サーバと AP の切断前は、クライアントは 802.1X 認証で認証されます。切断後はバックアップ用の PSK 認証で認証されます。

fail-permit template コマンドは、サービステンプレートが無効になっている場合にのみ実行でき、サービステンプレートが有効になった後に有効になります。

fail-permit template コマンドと **fail-permit enable** コマンドを同一のサービステンプレートに設定しないでください。

例

#サービステンプレートを障害許可サービステンプレートとして指定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] fail-permit template

関連コマンド

fail-permit enable

1.1.17 mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメイン名を指定します。設定範囲は 1～255 文字です。大文字と小文字を区別しません。

説明

mac-authentication domain コマンドはサービステンプレートで MAC 認証クライアントのための認証ドメインを指定します。

undo mac-authentication domain コマンドはデフォルトに戻します

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

MAC 認証は以下の順番で WLAN クライアントのための認証ドメインを選択します。

1) サービステンプレートで指定された認証ドメイン
2) system view で指定されたグローバル認証ドメイン
3) デフォルト認証ドメイン

例

サービステンプレート service1 で、MAC 認証クライアントのための認証ドメインとして my-domain を指定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] mac-authentication domain my-domain

1.1.18 mac-authentication max-user

Syntax

mac-authentication max-user *count*

undo mac-authentication max-user

デフォルト

512

View

Service template view

定義済みユーザロール

network-admin

パラメータ

count: 同時接続 MAC 認証クライアントの最大数を設定します。範囲は 1～512 です。

説明

mac-authentication max-user コマンドはサービステンプレートで MAC 認証クライアントの最大同時接続数を設定します。

undo mac-authentication max-user コマンドはデフォルトに戻します。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

最大数に達した場合、サービステンプレートは以降の MAC 認証クライアントを拒否します。

🕮 **メモ**:

- MAC 認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は、QX-W610 では 128 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

例

サービステンプレート service1 で、MAC 認証クライアントの最大接続数を 32 に設定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] mac-authentication max-user 32

目次

このセクションのページは **12-x-x** です。

2 章 WLAN IP スヌーピング 2-1
2.1 WLAN IP スヌーピング設定コマンド 2-1
2.1.1 client ipv4-snooping arp-learning enable 2-1
2.1.2 client ipv4-snooping dhcp-learning enable 2-1

2章 WLAN IP スヌーピング

2.1 WLAN IPスヌーピング設定コマンド

2.1.1 client ipv4-snooping arp-learning enable

Syntax

client ipv4-snooping arp-learning enable

undo client ipv4-snooping arp-learning enable

デフォルト

Snooping ARP packets は、有効

View

Service template view

定義済みユーザロール

network-admin

説明

client ipv4-snooping arp-learning enable コマンドは、スヌーピング ARP パケットを有効にします。

undo client ipv4-snooping arp-learning enable コマンドは、スヌーピング ARP パケットを無効にします。

例

ARP パケットのスヌーピングを無効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] undo client ipv4-snooping arp-learning enable

2.1.2 client ipv4-snooping dhcp-learning enable

Syntax

client ipv4-snooping dhcp-learning enable

undo client ipv4-snooping dhcp-learning enable

デフォルト

有効

View

Service template view

定義済みユーザロール

network-admin

説明

client ipv4-snooping dhcp-learning enable コマンドは、DHCPv4 パケットのスヌーピングを有効にします。

undo client ipv4-snooping dhcp-learning enable コマンドは、DHCPv4 パケットのスヌーピングを無効にします。

例

DHCPv4 snooping パケットを無効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] undo client ipv4-snooping dhcp-learning enable

目次

このセクションのページは **12-x-x** です。

3 章 AAA 3-1
3.1 AAA 設定コマンド 3-1
3.1.1 aaa session-limit 3-1
3.1.2 accounting default 3-2
3.1.3 accounting lan-access 3-4
3.1.4 accounting login 3-6
3.1.5 authentication default 3-8
3.1.6 authentication lan-access 3-10
3.1.7 authentication login 3-11
3.1.8 authorization command 3-14
3.1.9 authorization default 3-16
3.1.10 authorization lan-access 3-18
3.1.11 authorization login 3-20
3.1.12 display domain 3-22
3.1.13 domain 3-27
3.1.14 domain default enable 3-29
3.1.15 state (ISP domain view) 3-30
3.2 ローカルユーザ設定コマンド 3-31
3.2.1 access-limit 3-31
3.2.2 authorization-attribute (local user view/user group view) 3-32
3.2.3 bind-attribute 3-36
3.2.4 description (network access user view) 3-38
3.2.5 display local-user 3-39
3.2.6 display user-group 3-43
3.2.7 group 3-46
3.2.8 local-user 3-47
3.2.9 password (device management user view) 3-49
3.2.10 password (network access user view) 3-51
3.2.11 service-type (local user view) 3-52
3.2.12 state (local user view) 3-53
3.2.13 user-group 3-54
3.3 RADIUS 設定コマンド 3-55
3.3.1 accounting-on enable 3-55
3.3.2 data-flow-format (RADIUS scheme view) 3-56
3.3.3 display radius scheme 3-57
3.3.4 display radius statistics 3-62

3.3.5 key (RADIUS scheme view) 3-64
3.3.6 nas-ip (RADIUS scheme view) 3-66
3.3.7 primary accounting (RADIUS scheme view) 3-68
3.3.8 primary authentication (RADIUS scheme view) 3-70
3.3.9 radius dscp 3-72
3.3.10 radius nas-ip 3-73
3.3.11 radius scheme 3-75
3.3.12 radius-server test-profile 3-76
3.3.13 reset radius statistics 3-77
3.3.14 retry 3-77
3.3.15 retry realtime-accounting 3-79
3.3.16 secondary accounting (RADIUS scheme view) 3-81
3.3.17 secondary authentication (RADIUS scheme view) 3-84
3.3.18 state primary 3-86
3.3.19 state secondary 3-87
3.3.20 timer quiet (RADIUS scheme view) 3-89
3.3.21 timer realtime-accounting (RADIUS scheme view) 3-90
3.3.22 timer response-timeout (RADIUS scheme view) 3-92
3.3.23 user-name-format (RADIUS scheme view) 3-94

3章 AAA

3.1 AAA設定コマンド

3.1.1 aaa session-limit

Syntax

aaa session-limit { **ftp** | **http** | **https | ssh** | **telnet** } *max-sessions*

undo aaa session-limit { **ftp** | **http** | **https | ssh** | **telnet** }

デフォルト

32

View

System view

定義済みユーザロール

network-admin

パラメータ

ftp: FTP ユーザを指定します。

http: HTTP ユーザを指定します。

https: HTTPS ユーザを指定します。

ssh: SSH ユーザを指定します。

telnet: Telnet ユーザを指定します。

max-sessions: 装置に同時に接続可能な最大接続数を指定します。FTP、SSH、Telnet の設定範囲は 1～32 です。HTTP、HTTPS の設定範囲は 1～64 です。

説明

aaa session-limit コマンドは、装置に同時に接続可能な最大接続数を指定します。

undo aaa session-limit コマンドは、デフォルトに戻します。

ユーザタイプの最大同時接続数が上限に到達したのち、システムは後続のユーザタイプの接続を拒否します。

例

FTP ユーザの最大同時接続数を 4 に設定します。

<AP> system-view

[AP] aaa session-limit ftp 4

3.1.2 accounting default

Syntax

accounting default { **local** [**radius-scheme** radius-scheme-name] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting default

デフォルト

local

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカルアカウンティングを実行します。

none: アカウンティングを実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1 ～32 です。大文字、小文字を区別しません。

説明

accounting default コマンドは ISP ドメインのデフォルトアカウンティング方式を指定します。

undo accounting default コマンドはデフォルトに戻します。

デフォルトアカウンティング方式は、この方式をサポートするすべてのユーザで使用されます。特定のアカウンティング方式は設定されません。

ローカルアカウンティングは、ローカルユーザ接続の数を監視し、制御するためにのみ使用されます。アカウンティング機能が一般的に提供する統計機能を提供していません。

1 つのプライマリデフォルトアカウンティング方式と複数のバックアップのアカウンティング方式を指定することができます。

プライマリアカウンティングが無効であるとき、装置は、順番にバックアップのアカウンティング方式を使用します。たとえば、**accounting default radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS アカウンティング方式と 2 つのバックアップの方式（ローカルアカウンティング方式とアカウンティングがない方式）を指定します。装置はデフォルトで RADIUS アカウンティング方式を実行し、RADIUS サーバが無効であるときローカルアカウンティング方式を実行します。RADIUS アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

リモートアカウンティング方式は、次の状況では無効です。

- 指定されたアカウンティングスキームは存在しません。
- アカウンティングパケットの送信に失敗しました。
- 装置は、アカウンティングサーバからアカウンティング応答パケットを受信しません。

装置が一致するローカルユーザ設定を見つけられなかった場合、ローカルアカウンティング方式は無効になります。

プライマリアカウンティング方式がローカルの場合、ユーザのアカウンティングには次の規則が適用されます。

- 装置は、ローカルアカウンティングが無効な場合にのみ、次のいずれかの理由でバックアップアカウンティング方式を順番に使用します。
  - □ ローカルアカウンティングプロセスで例外が発生しました。
  - □ 装置でユーザーアカウントが設定されていないか、ユーザにアクセスサービスの使用が許可されていません。
- その他の理由でローカルアカウンティングが無効な場合、デバイスはバックアップアカウンティング方式に切り替えません。ユーザのアカウンティングは失敗します。

例

ISP ドメイン test のデフォルトアカウンティング方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルとして設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] accounting default radius-scheme rd local

関連コマンド

- **local-user**
- **radius scheme**

3.1.3 accounting lan-access

Syntax

accounting lan-access { **broadcast radius-scheme** *radius-scheme-name1* **radius-scheme** *radius-scheme-name2* [**local**] [**none**] | **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting lan-access

デフォルト

LAN ユーザのアカウンティング方式はデフォルトアカウンティング方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

broadcast: RADIUS スキームのサーバにアカウンティング要求をブロードキャストします。

radius-scheme *radius-scheme-name1:* プライマリブロードキャスト RADIUS スキームを名前で指定します。名前は大文字と小文字を区別せず、1〜32 文字の文字列で指定します。

radius-scheme *radius-scheme-name 2*: バックアップブロードキャスト 32 RADIUS スキームを名前で指定します。

local: ローカルアカウンティングを実行します。

none: アカウンティングを実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキームを指定します。設定範囲は 1〜32 です。大文字、小文字を区別しません。

説明

accounting lan-access コマンドは LAN ユーザのアカウンティング方式を設定します。

undo accounting lan-access コマンドはデフォルトに戻します。

1 つのプライマリアカウンティング方式と複数のバックアップのアカウンティング方式を指定することができます。

プライマリアカウンティングが無効であるとき、装置は、順番にバックアップのアカウンティング方式を使用します。たとえば、**accounting lan-access radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリ RADIUS アカウンティング方式と 2 つのバックアップ方式（ローカルアカウンティング方式とアカウンティングがない

方式）を指定します。装置はデフォルトで RADIUS アカウンティング方式を実行し、RADIUS サーバが無効であるときローカルアカウンティング方式を実行します。RADIUS アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

リモートアカウンティング方式は、次の状況では無効です。

- 指定されたアカウンティングスキームは存在しません。
- アカウンティングパケットの送信に失敗しました。
- 装置は、アカウンティングサーバからアカウンティング応答パケットを受信しません。

装置が一致するローカルユーザ設定を見つけられなかった場合、ローカルアカウンティング方式は無効になります。

プライマリアカウンティング方式がローカルの場合、ユーザのアカウンティングには次の規則が適用されます。

- 装置は、ローカルアカウンティングが無効な場合にのみ、次のいずれかの理由でバックアップアカウンティング方式を順番に使用します。
  - ローカルアカウンティングプロセスで例外が発生しました。
  - 装置でユーザーアカウントが設定されていないか、ユーザにアクセスサービスの使用が許可されていません。
- その他の理由でローカルアカウンティングが無効な場合、デバイスはバックアップアカウンティング方式に切り替えません。ユーザのアカウンティングは失敗します。

例

ISP ドメイン test の LAN ユーザのローカルアカウンティング方式を設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] accounting lan-access local

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

<AP> system-view

[AP] domain test

[AP-isp-test] accounting lan-access radius-scheme rd local

関連コマンド

- **accounting default**
- **local-user**
- **radius scheme**

3.1.4 accounting login

Syntax

accounting login { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo accounting login

デフォルト

ログインユーザの ISP ドメインのアカウンティング方式はデフォルトアカウンティング方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカルアカウンティングを実行します。

none: アカウンティングを実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

accounting login コマンドはログインユーザのアカウンティング方式を指定します。

undo accounting login コマンドはデフォルトに戻します。

FTP、SFTP ユーザのアカウンティングはサポートしていません。

1 つのプライマリアカウンティング方式と複数のバックアップのアカウンティング方式を指定することができます。

プライマリアカウンティングが無効であるとき、装置は、順番にバックアップのアカウンティング方式を使用します。たとえば、**accounting login radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS アカウンティング方式と 2 つのバックアップ方式（ローカルアカウンティング方式とアカウンティングがない方式）を指定します。装置はデフォルトで RADIUS アカウンティング方式を実行し、RADIUS サーバが無効であるときローカルアカウンティング方式を実行します。RADIUS アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

リモートアカウンティング方式は、次の状況では無効です。

- 指定されたアカウンティングスキームは存在しません。
- アカウンティングパケットの送信に失敗しました。

- 装置は、アカウンティングサーバからアカウンティング応答パケットを受信しません。

装置が一致するローカルユーザ設定を見つけられなかった場合、ローカルアカウンティング方式は無効になります。

プライマリアカウンティング方式がローカルの場合、ユーザのアカウンティングには次の規則が適用されます。

- 装置は、ローカルアカウンティングが無効な場合にのみ、次のいずれかの理由でバックアップアカウンティング方式を順番に使用します。
  - ローカルアカウンティングプロセスで例外が発生しました。
  - 装置でユーザーアカウントが設定されていません。
- その他の理由でローカルアカウンティングが無効な場合、デバイスはバックアップアカウンティング方式に切り替えません。ユーザのアカウンティングは失敗します。

例

ISP ドメイン test のログインユーザのローカルアカウンティングを設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] accounting login local

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

<AP> system-view

[AP] domain test

[AP-isp-test] accounting login radius-scheme rd local

関連コマンド

- **accounting default**
- **local-user**
- **radius scheme**

3.1.5 authentication default

Syntax

authentication default { **ldap-scheme** ldap-scheme-name [**local**] [**none**] | **local** [**radius-scheme** radius-scheme-name] [**none**] | **local** [**ldap-scheme** ldap-scheme-name] [**none**] | **none** | **radius-scheme** radius-scheme-name [**local**] [**none**] }

undo authentication default

デフォルト

local

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

ldap-scheme *ldap-scheme-name*: LDAP スキームを名前で指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

local: ローカル認証を実行します。

none: 認証を実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authentication default コマンドは ISP ドメインのデフォルト認証方式を指定します。

undo authentication default コマンドはデフォルトに戻します。

デフォルト認証方式は、この方式をサポートするすべてのユーザで使用されます。特定の認証方式は設定されません。

1 つのプライマリデフォルト認証方式と複数のバックアップの認証方式を指定することができます。

プライマリ認証が無効であるとき、装置は、順番にバックアップの認証方式を使用します。たとえば、**authentication default radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 認証方式と 2 つのバックアップの方式（ローカル認証方式と認証がない方式）を指定します。装置はデフォルトで RADIUS 認証方式を実行し、RADIUS サーバが無効であるときローカル認証方式を実行します。RADIUS 認証方式とローカル認証方式の両方が無効であるとき、装置は認証を実行しません。

アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

リモートアカウンティング方式は、次の状況では無効です。

- 指定されたアカウンティングスキームは存在しません。
- アカウンティングパケットの送信に失敗しました。
- 装置は、アカウンティングサーバからアカウンティング応答パケットを受信しません。

装置が一致するローカルユーザ設定を見つけられなかった場合、ローカルアカウンティング方式は無効になります。

プライマリアカウンティング方式がローカルの場合、ユーザのアカウンティングには次の規則が適用されます。

- 装置は、ローカルアカウンティングが無効な場合にのみ、次のいずれかの理由でバックアップアカウンティング方式を順番に使用します。
  - ローカルアカウンティングプロセスで例外が発生しました。
  - 装置でユーザーアカウントが設定されていないか、ユーザにアクセスサービスの使用が許可されていません。
- その他の理由でローカルアカウンティングが無効な場合、装置はバックアップアカウンティング方式に切り替えません。ユーザのアカウンティングは失敗します。

例

ISP ドメイン test のデフォルト認証方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルとして設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authentication default radius-scheme rd local

関連コマンド

- **local-user**
- **radius scheme**

3.1.6 authentication lan-access

Syntax

authentication lan-access { **ldap-scheme** *ldap-scheme-name* [**local**] [**none**] | **local** [**ldap-scheme** *ldap-scheme-name* | **radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authentication lan-access

デフォルト

LAN ユーザの認証方式はデフォルト認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

ldap-scheme *ldap-scheme-name*: LDAP スキームを名前で指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

local: ローカル認証を実行します。

none: 認証を実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authentication lan-access コマンドは LAN ユーザの認証方式を設定します。

undo authentication lan-access コマンドはデフォルトに戻します。

1 つのプライマリ認証方式と複数のバックアップの認証方式を指定することができます。

プライマリ認証が無効であるとき、装置は、順番にバックアップの認証方式を使用します。たとえば、**authentication lan-access radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリ RADIUS 認証方式と 2 つのバックアップ方式（ローカル認証方式と認証がない方式）を指定します。装置はデフォルトで RADIUS 認証方式を実行し、RADIUS サーバが無効であるときローカル認証方式を実行します。RADIUS 認証方式とローカル認証方式の両方が無効であるとき、装置は認証を実行しません。

アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

リモートアカウンティング方式は、次の状況では無効です。

- 指定されたアカウンティングスキームは存在しません。
- アカウンティングパケットの送信に失敗しました。

- 装置は、アカウンティングサーバからアカウンティング応答パケットを受信しません。

装置が一致するローカルユーザ設定を見つけられなかった場合、ローカルアカウンティング方式は無効になります。

プライマリアカウンティング方式がローカルの場合、ユーザのアカウンティングには次の規則が適用されます。

- 装置は、ローカルアカウンティングが無効な場合にのみ、次のいずれかの理由でバックアップアカウンティング方式を順番に使用します。
  - ローカルアカウンティングプロセスで例外が発生しました。
  - 装置でユーザーアカウントが設定されていないか、ユーザにアクセスサービスの使用が許可されていません。
- その他の理由でローカルアカウンティングが無効な場合、装置はバックアップアカウンティング方式に切り替えません。ユーザのアカウンティングは失敗します。

例

ISP ドメイン test の LAN ユーザのローカル認証方式を設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authentication lan-access local

LAN ユーザの ISP ドメイン test の認証方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authentication lan-access radius-scheme rd local

関連コマンド

- **authentication default**
- **local-user**
- **radius scheme**

3.1.7 authentication login

Syntax

authentication login { **ldap-scheme** ldap-scheme-name [**local**] [**none**] | **local** [**ldap-scheme** ldap-scheme-name | **radius-scheme** radius-scheme-name] [**none**] | **none** | **radius-scheme** radius-scheme-name [**local**] [**none**] }

undo authentication login

デフォルト

ログインユーザの ISP ドメインの認証方式はデフォルト認証方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

ldap-scheme *ldap-scheme-name*: LDAP スキームを名前で指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

local: ローカル認証を実行します。

none: 認証を実行しません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authentication login コマンドはログインユーザの認証方式を指定します。

undo authentication login コマンドはデフォルトに戻します。

1 つのプライマリ認証方式と複数のバックアップの認証方式を指定することができます。

プライマリ認証が無効であるとき、装置は、順番にバックアップの認証方式を使用します。たとえば、**authentication login radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 認証方式と 2 つのバックアップ方式（ローカル認証方式と認証がない方式）を指定します。装置はデフォルトで RADIUS 認証方式を実行し、RADIUS サーバが無効であるときローカル認証方式を実行します。RADIUS 認証方式とローカル認証方式の両方が無効であるとき、装置は認証を実行しません。

アカウンティング方式とローカルアカウンティング方式の両方が無効であるとき、装置はアカウンティング方式を実行しません。

リモートアカウンティング方式は、次の状況では無効です。

- 指定されたアカウンティングスキームは存在しません。
- アカウンティングパケットの送信に失敗しました。
- 装置は、アカウンティングサーバからアカウンティング応答パケットを受信しません。

装置が一致するローカルユーザ設定を見つけられなかった場合、ローカルアカウンティング方式は無効になります。

プライマリアカウンティング方式がローカルの場合、ユーザのアカウンティングには次の規則が適用されます。

- 装置は、ローカルアカウンティングが無効な場合にのみ、次のいずれかの理由でバックアップアカウンティング方式を順番に使用します。
  - ローカルアカウンティングプロセスで例外が発生しました。
  - 装置でユーザーアカウントが設定されていないか、ユーザにアクセスサービスの使用が許可されていません。
- その他の理由でローカルアカウンティングが無効な場合、装置はバックアップアカウンティング方式に切り替えません。ユーザのアカウンティングは失敗します。

例

ISP ドメイン test のログインユーザのローカル認証を設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authentication login local

ログインユーザの ISP ドメイン test の認証方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authentication login radius-scheme rd local

関連コマンド

- **authentication default**
- **local-user**
- **radius scheme**

3.1.8 authorization command

Syntax

authorization command { **local** [**none**] | **none** }

undo authorization command

デフォルト

ISP ドメインのコマンド許可（認可）方式はデフォルト許可方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。許可サーバは、入力されたコマンドがユーザロールで許可されているかどうかを確認しません。ユーザロールがコマンドを許可している場合、コマンドが正常に実行されます。

説明

authorization command コマンドはコマンドの許可方式を指定します。

undo authorization command コマンドはデフォルトに戻します。

入力された各コマンドが許可されているかどうか確認するため、コマンド許可は、許可サーバを使用しログインユーザが入力可能なコマンドのみを実行できるように制限します。

ローカルコマンド許可が設定されているとき、装置は入力された各コマンドとユーザの設定を比較します。ユーザの許可されたユーザロールによって許可されるときのみ、コマンドが実行されます。

実行できるコマンドは、ユーザロールのアクセス許可と許可サーバのコマンド許可の両方で管理されます。アクセス許可の管理は、許可されたユーザロールが入力されたコマンドにアクセスできるかどうかを管理しますが、ユーザロールがこれらのコマンドに許可を取得したかどうかを管理しません。コマンドがアクセス許可によって許可されるが、コマンド許可で許可されていない場合、コマンドは実行できません。

1 つのプライマリコマンド許可方式と複数のバックアップのコマンド許可方式を指定することができます。

デフォルト許可方式が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization command local none** コマンドはプライマリデフォルトローカル許可方式と 1 つのバックアップ方式（認証がない方式）を指定します。装置

はデフォルトでローカル許可方式を実行し、ローカル許可方式が無効であるとき装置は許可を実行しません。

リモート許可方式は、次の状況では無効です。

- 指定された許可スキームが存在しません。
- 許可パケットの送信が失敗します。
- 装置は、許可サーバから許可応答パケットを受信しません。装置が一致するローカルユーザ設定を見つけられなかった場合、ローカル許可方式は無効になります。

例

ISP ドメイン test の LAN ユーザのローカルコマンド許可方式を設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authorization command local

ログインユーザの ISP ドメイン test の認証方式を設定します。プライマリをローカル許可方式、バックアップをコマンド許可なしに設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authorization command local none

関連コマンド

local-user

3.1.9 authorization default

Syntax

authorization default { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization default

デフォルト

local

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。ユーザが認証にパスしたのち、以下のデフォルト許可情報を適用します。

- ログインユーザがネットワークにアクセスできません。
- ログインユーザはユーザロール Level-0 に割り当てられています。ログインユーザは Telnet、FTP、SFTP、端末ユーザです。端末ユーザはコンソールポートを使用して装置にアクセスできます。
- FTP、SFTP ユーザが作業ディレクトリとして設定した NAS のルートディレクトリを持っていますが、ユーザはルートディレクトリへのアクセス権限がありません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authorization default コマンドは ISP ドメインのデフォルト許可方式を指定します。

undo authorization default コマンドはデフォルトに戻します。

デフォルト許可方式は、この方式をサポートするすべてのユーザで使用されます。特定の許可方式は設定されません。

ISP ドメインの認証方式と許可方式が同じ RADIUS スキームを使用するときのみ RADIUS 許可が適用されます。

1 つのプライマリデフォルト許可方式と複数のバックアップの許可方式を指定することができます。

プライマリ許可が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization default radius-scheme** *radius-scheme-name* **local none**

コマンドはプライマリデフォルト RADIUS 許可方式と 2 つのバックアップの方式（ローカル許可方式と許可がない方式）を指定します。装置はデフォルトで RADIUS 許可方式を実行し、RADIUS サーバが無効であるときローカル許可方式を実行します。RADIUS 許可方式とローカル許可方式の両方が無効であるとき、装置は許可を実行しません。

リモート許可方式は、次の状況では無効です。

- 指定された許可スキームが存在しません。
- 許可パケットの送信が失敗します。
- 装置は、許可サーバから許可応答パケットを受信しません。装置が一致するローカルユーザ設定を見つけられなかった場合、ローカル許可方式は無効になります。

装置が一致するローカルユーザ設定を見つけられなかった場合、ローカルアカウンティング方式は無効になります。

プライマリアカウンティング方式がローカルの場合、ユーザのアカウンティングには次の規則が適用されます。

- 装置は、ローカルアカウンティングが無効な場合にのみ、次のいずれかの理由でバックアップアカウンティング方式を順番に使用します。
  - ローカルアカウンティングプロセスで例外が発生しました。
  - 装置でユーザーアカウントが設定されていないか、ユーザにアクセスサービスの使用が許可されていません。
- その他の理由でローカルアカウンティングが無効な場合、装置はバックアップアカウンティング方式に切り替えません。ユーザのアカウンティングは失敗します。

例

ISP ドメイン test のデフォルト許可方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルとして設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authorization default radius-scheme rd local

関連コマンド

- **local-user**
- **radius scheme**

3.1.10 authorization lan-access

Syntax

authorization lan-access { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization lan-access

デフォルト

LAN ユーザの許可方式はデフォルト許可方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。認証された LAN ユーザは直接ネットワークにアクセスします。

radius-scheme *radius-scheme-name*: RADIUS スキームを指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authorization lan-access コマンドは LAN ユーザの許可方式を設定します。

undo authorization lan-access コマンドはデフォルトに戻します。

ISP ドメインの認証方式と許可方式が同じ RADIUS スキームを使用するときのみ RADIUS 許可が適用されます。

1 つのプライマリ許可方式と複数のバックアップの許可方式を指定することができます。

プライマリ許可が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization lan-access radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリ RADIUS 許可方式と 2 つのバックアップ方式（ローカル許可方式と許可がない方式）を指定します。装置はデフォルトで RADIUS 許可方式を実行し、RADIUS サーバが無効であるときローカル許可方式を実行します。RADIUS 許可方式とローカル許可方式の両方が無効であるとき、装置は許可を実行しません。

リモート許可方式は、次の状況では無効です。

- 指定された許可スキームが存在しません。
- 許可パケットの送信が失敗します。
- 装置は、許可サーバから許可応答パケットを受信しません。装置が一致するローカルユーザ設定を見つけられなかった場合、ローカル許可方式は無効になります。

装置が一致するローカルユーザ設定を見つけられなかった場合、ローカルアカウンティング方式は無効になります。

プライマリアカウンティング方式がローカルの場合、ユーザのアカウンティングには次の規則が適用されます。

- 装置は、ローカルアカウンティングが無効な場合にのみ、次のいずれかの理由でバックアップアカウンティング方式を順番に使用します。
  - ローカルアカウンティングプロセスで例外が発生しました。
  - 装置でユーザーアカウントが設定されていないか、ユーザにアクセスサービスの使用が許可されていません。
- その他の理由でローカルアカウンティングが無効な場合、装置はバックアップアカウンティング方式に切り替えません。ユーザのアカウンティングは失敗します。

例

ISP ドメイン test の LAN ユーザのローカル許可方式を設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authorization lan-access local

LAN ユーザの ISP ドメイン test の許可方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authorization lan-access radius-scheme rd local

関連コマンド

- **authorization default**
- **local-user**
- **radius scheme**

3.1.11 authorization login

Syntax

authorization login { **local** [**radius-scheme** *radius-scheme-name*] [**none**] | **none** | **radius-scheme** *radius-scheme-name* [**local**] [**none**] }

undo authorization login

デフォルト

ログインユーザの ISP ドメインの許可方式はデフォルト許可方式を使用します。

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

local: ローカル許可を実行します。

none: 許可を実行しません。ユーザが認証にパスしたのち、以下のデフォルト許可情報を適用します。

- ログインユーザはユーザロール Level-0 に割り当てられています。ログインユーザは Telnet、FTP、SFTP、端末ユーザです。端末ユーザはコンソールポートを使用して装置にアクセスできます。
- FTP、SFTP ユーザが作業ディレクトリとして設定した NAS のルートディレクトリを持っていますが、ユーザはルートディレクトリへのアクセス権限がありません。

radius-scheme *radius-scheme-name*: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

authorization login コマンドはログインユーザの許可方式を指定します。

undo authorization login コマンドはデフォルトに戻します。

ISP ドメインの認証方式と許可方式が同じ RADIUS スキームを使用するときのみ RADIUS 許可が適用されます。

1 つのプライマリ許可方式と複数のバックアップの許可方式を指定することができます。

プライマリ許可が無効であるとき、装置は、順番にバックアップの許可方式を使用します。たとえば、**authorization login radius-scheme** *radius-scheme-name* **local none** コマンドはプライマリデフォルト RADIUS 許可方式と 2 つのバックアップ方式（ローカル許可方式と許可がない方式）を指定します。装置はデフォルトで RADIUS 許可方式を実行し、RADIUS サーバが無効であるときローカル許可方式を実行します。RADIUS 許可方式とローカル許可方式の両方が無効であるとき、装置は許可を実行しません。

リモート許可方式は、次の状況では無効です。

- 指定された許可スキームが存在しません。
- 許可パケットの送信が失敗します。
- 装置は、許可サーバから許可応答パケットを受信しません。装置が一致するローカルユーザ設定を見つけられなかった場合、ローカル許可方式は無効になります。

装置が一致するローカルユーザ設定を見つけられなかった場合、ローカルアカウンティング方式は無効になります。

プライマリアカウンティング方式がローカルの場合、ユーザのアカウンティングには次の規則が適用されます。

- 装置は、ローカルアカウンティングが無効な場合にのみ、次のいずれかの理由でバックアップアカウンティング方式を順番に使用します。
  - ローカルアカウンティングプロセスで例外が発生しました。
  - 装置でユーザーアカウントが設定されていないか、ユーザにアクセスサービスの使用が許可されていません。
- その他の理由でローカルアカウンティングが無効な場合、装置はバックアップアカウンティング方式に切り替えません。ユーザのアカウンティングは失敗します。

例

ISP ドメイン test のログインユーザのローカル許可を設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authorization login local

ログインユーザの ISP ドメイン test の許可方式を設定します。プライマリを RADIUS スキーム rd、バックアップをローカルに設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] authorization login radius-scheme rd local

関連コマンド

- **authorization default**
- **local-user**
- **radius scheme**

3.1.12 display domain

Syntax

display domain [*isp-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。ISP ドメインを指定しない場合、すべての ISP ドメインの設定を表示します。

説明

display domain コマンドは ISP ドメインの設定を表示します。

例

すべての ISP ドメインの設定を表示します。

<AP> display domain

```
Total 2 domains

Domain: system
  State: Active
  Default authentication scheme:  Local
  Default authorization  scheme:  Local
  Default accounting    scheme:  Local
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  Service type: HSI
  Session time: Exclude idle time
  NAS-ID: N/A
  Authorization attributes:
    Idle cut: Disabled
    IGMP access number: 4
    MLD access number:  4

Domain: dm
```

```
  State: Active
  Login  authentication scheme:  RADIUS=rad
  Login  authorization  scheme:  HWTACACS=hw
  Super  authentication scheme:  RADIUS=rad
  Command authorization  scheme:  HWTACACS=hw
  LAN access authentication scheme:  RADIUS=r4
  PPP    accounting    scheme:  RADIUS=r1, (RADIUS=r2), HWTACACS=tc, Local
  Portal  authentication scheme:  LDAP=ldp
  Default authentication scheme:  LDAP=rad, Local, None
  Default authorization  scheme:  Local
  Default accounting    scheme:  None
  Accounting start failure action: Online
  Accounting update failure action: Online
  Accounting quota out action: Offline
  ITA service poilcy: ita1
  Service type: HSI
  Session time: Include idle time
  NAS-ID: test
  Authorization attributes:
    Idle cut : Enabled
      Idle timeout: 2 minutes
      Flow: 10240 bytes
    Session timeout: 34 minutes
    IP pool: appy
    User profile: test
    Inbound CAR: CIR 64000 bps PIR 640000 bps
    Outbound CAR: CIR 64000 bps PIR 640000 bps
    ACL number: 3000
    User group: ugg
    Primary DNS server: 6.6.6.6
    Secondary DNS server: 3.6.2.3
    URL: http://portal
    IGMP access number: 12
    MLD access number: 35

Default domain name: system
```

表 3-1 コマンド出力

フィールド	説明
Total 2 domains	ドメインの総数です。
Domain	ISP ドメイン名です。

フィールド	説明
State	ISP ドメインの状態です。
Default authentication scheme	デフォルト認証方式です。
Default authorization scheme	デフォルト許可方式です。
Default accounting scheme	デフォルトアカウンティング方式です。
Login authentication scheme	ログインユーザの認証方式です。
Login authorization scheme	ログインユーザの許可方式です。
Login accounting scheme	ログインユーザのアカウンティング方式です。
Super authentication scheme	装置に再接続を行わず別のユーザロールを取得する認証方式です。
PPP authentication scheme	PPPユーザの認証方式です。
PPP authorization scheme	PPPユーザの認可方式です。
PPP accounting scheme	PPPユーザのアカウンティング方式です。
Command authorization scheme	コマンドライン許可方式です。
LAN access authentication scheme	LANユーザの認証方式です。
LAN access authorization scheme	LANユーザの許可方式です。
LAN access accounting scheme	LANユーザのアカウンティング方式です。
Portal authentication scheme	ポータルユーザの認証方式。
Portal authorization scheme	ポータルユーザの認可方式。
Portal accounting scheme	ポータルユーザのアカウンティング方法。
IKE authentication scheme	IKE拡張認証方式。
IKE authorization scheme	IKE拡張認証の認可方式。
RADIUS	RADIUSスキームです。
HWTACACS	HWTACACSスキームです。 HWTACACSスキームはサポートしていません。
LDAP	LDAPスキームです。 LDAPスキームはサポートしていません。

フィールド	説明
Local	ローカルスキームです。
None	認証、許可、アカウンティングがありません。
Accounting start failure action	アカウンティング開始の失敗となるユーザのアクセス制御です。 • **Online**–ユーザがオンライン状態のままとなることを許可します。 • **Offline**–ユーザをログオフします。
Accounting update failure max-times	ドメインの各ユーザによって、許可されたアカウンティングアップデートが連続して失敗する最大数です。
Accounting update failure action	すべてのアカウンティングアップデート試行に失敗したユーザのアクセス制御です。 • **Online**–ユーザがオンライン状態のままとなることを許可します。 • **Offline**–ユーザをログオフします。
Accounting quota out action	データ割り当てを使い果たしたユーザの制御です。 • **Online**–ユーザがオンライン状態のままとなることを許可します。 • **Offline**–ユーザをログオフします。
Service type	ISPドメインのサービスタイプです。HIS、STB、VoIPがあります。
Session time	接続失敗あるいは誤動作によって、ユーザがオフラインとなったため、オンライン時間がサーバに送信されました。 • **Include idle time**–オンライン時間にアイドルカット期間が含まれます。 • **Exclude idle time**–オンライン時間にアイドルカット期間が含まれません。
User address type	ISPドメイン内のユーザのIPアドレスのタイプです。
NAS-ID	デバイスのNAS-IDです。ISPドメインにNAS-IDが設定されていない場合、このフィールドにはN/Aが表示されます。
Idle cut	アイドルカット機能の状態です。 • **Enabled**—アイドルカット機能は有効です。アイドルタイムアウト時間に最小のトラフィック要件を満たしていないユーザをログオフします。 • **Disabled**—アイドルカット機能は無効です。
Idle timeout	アイドルタイムアウト時間 (分単位) です。

フィールド	説明
Flow	ログインユーザがアイドルタイムアウト期間に生成する必要がある最小トラフィック (バイト単位) です。
Session timeout	ISPドメイン内のユーザのセッションタイムアウト時間 (分単位) です 。
IP pool	認可IPv 4アドレスプールの名前です。
User profile	許可ユーザプロファイル名です。
Inbound CAR	認可インバウンドCARです。 • **CIR** —Committed 情報レート (bps 単位)。 • **PIR**—ピーク情報レート (bps 単位)。
Outbound CAR	認可アウトバウンドCARです。 • **CIR** —Committed 情報レート (bps 単位)。 • **PIR**—ピーク情報レート (bps 単位)。
ACL number	ユーザの許可ACLです。
User group	ユーザの許可ユーザグループです。
Primary DNS server	ユーザの認可プライマリDNSサーバのIPv 4アドレスです。
Secondary DNS server	ユーザの認可セカンダリDNSサーバのIPv 4アドレスです。
URL	ユーザのリダイレクトURLです。
IGMP max access number	IPv4ユーザが同時に加入できるIGMPグループの最大数です。
Default domain name	コマンドライン許可方式です。

3.1.13 domain

Syntax

domain *isp-name*

undo domain *isp-name*

デフォルト

domain name は、system

View

System view

定義済みユーザロール

network-admin

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。

次の記号は使用できません。スラッシュ（/），バックスラッシュ、垂直バー（|）、コーテーションマーク（"）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）

次のドメイン名は使用できません。(d)、(de) (def)、(defa)、(defau)、(defaul)、(default)、(i)、(if)、(if-)、(if-u)、(if-un)、(if-unk)、(if-unkn)、(if-unkno)、(if-unknow)、(if-unknown)

説明

domain コマンドは ISP ドメインを作成し、ISP domain view に移行します。ISP ドメインが既に存在する場合、その view に移行します。

undo domain コマンドは ISP ドメインを削除します。

作成されたとき、すべての ISP ドメインはアクティブ状態です。

システムには予約済み ISP ドメイン system があり、修正できますが削除することはできません。

デフォルト ISP ドメインは、削除することができません。**undo domain** コマンドを使用する前に、**undo domain default enable** コマンドを使用して、デフォルトでない ISP ドメインを変更してください。

ドメイン名を含むユーザ名は、異なるタイプのユーザの最大長を超過しないように短いユーザ名を使用してください。

例

ISP ドメイン test を作成し、ISP domain view に移行します。

<AP> system-view

[AP] domain test

[AP-isp-test]

関連コマンド

- **display domain**
- **domain default enable**
- **state (ISP domain view)**

3.1.14 domain default enable

Syntax

domain default enable *isp-name*

undo domain default enable

デフォルト

system

View

System view

定義済みユーザロール

network-admin

パラメータ

isp-name: ISP ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。

説明

domain default enable コマンドはデフォルト ISP ドメインを指定します。ドメイン名が付加されないユーザは、デフォルトドメインであるとみなします。

undo domain default enable コマンドはデフォルトに戻します。

デフォルトの ISP ドメインは 1 つしかありません。

デフォルトの ISP ドメインは、削除することができません。**undo domain** コマンドを使用する前に、**undo domain default enable** コマンドを使用して、デフォルトでない ISP ドメインを変更してください。

例

ISP ドメイン test を作成し、デフォルト ISP ドメインとして設定します。

<AP> system-view

[AP] domain test

[AP-isp-test] quit

[AP] domain default enable test

関連コマンド

- **display domain**
- **domain**

3.1.15 state (ISP domain view)

Syntax

state { **active** | **block** }

undo state

デフォルト

active

View

ISP domain view

定義済みユーザロール

network-admin

パラメータ

active: ISP ドメインをアクティブ状態にし、ISP ドメイン内のユーザがネットワークサービスを要求できるようにします。

block: ISP ドメインをブロック状態にし、ISP ドメイン内のユーザがネットワークサービスを要求できないようにします。

説明

state コマンドは ISP ドメインの状態を設定します。

undo state コマンドはデフォルトに戻します。

ISP ドメインをブロック状態にすると、このドメイン内のオフラインのユーザは、ネットワークサービスを要求できなくなります。オンラインユーザには影響しません。

例

ISP ドメイン test をブロック状態にします。

<AP> system-view

[AP] domain test

[AP-isp-test] state block

関連コマンド

display domain

3.2 ローカルユーザ設定コマンド

3.2.1 access-limit

Syntax

access-limit *max-user-number*

undo access-limit

デフォルト

ローカルユーザを使用して同時に接続するユーザ数に制限はありません。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

max-user-number: 同時に接続するユーザの最大数です。設定範囲は 1～1024 です。

説明

access-limit コマンドはローカルユーザを使用して同時に接続するユーザの最大数を設定します。

undo access-limit コマンドはデフォルトに戻します。

ローカルユーザでローカルアカウンティングが設定されているときのみ適用されます。

FTP、SFTP ユーザはアカウンティングをサポートしていないため、FTP、SFTP ユーザには適用されません。

例

ローカルユーザ abc を使用して同時に接続するユーザの最大数 5 を設定します。

<AP> system-view

[AP] local-user abc

[AP-luser-manage-abc] access-limit 5

関連コマンド

display local-user

3.2.2 authorization-attribute (local user view/user group view)

Syntax

authorization-attribute { **acl** acl-number | **callback-number** callback-number | **idle-cut** minutes | **ip** ipv4-address | **ip-pool** ipv4-pool-name | { **primary-dns** | **secondary-dns** } { **ip** ipv4-address } | **session-timeout** minutes | url url-string | **user-profile** profile-name | **user-role** role-name | **vlan** vlan-id | **work-directory** directory-name } *

undo authorization-attribute { **acl** | **callback-number** | **idle-cut** | **ip** | **ip-pool** | **primary-dns** | **secondary-dns** | **session-timeout** | **url** | **user-profile** | **user-role** role-name | **vlan** | **work-directory** } *

デフォルト

FTP、SFTPユーザは作業ディレクトリとしてNASのルートディレクトリを設定します。しかし、ユーザはルートディレクトリへのアクセス許可がありません。

network-admin あるいは level-15 のユーザによって作成されたローカルユーザは network-operator のユーザロールが割り当てられています。

View

Local user view

User group view

定義済みユーザロール

network-admin

パラメータ

acl *acl-number*: 許可 ACL を指定します。設定範囲は 2000～5999 です。認証をパスした後、ローカルユーザは ACL で指定されたネットワークリソースにアクセスすることができます。

callback-number *callback-number*: 許可された PPP コールバック番号を指定します。*callback-number* 引数は、1 から 64 文字の大文字と小文字を区別する文字列です。ローカルユーザが認証に合格すると、装置はこの番号を使用してユーザを呼び出します。

idle-cut *minute*: アイドルタイムアウト時間を設定します。設定範囲は 1～120 分です。指定されるアイドル時間を超過したアイドル中のオンラインユーザはログアウトされます。

ip *ipv4-address*: 認証を通過したユーザにスタティック IPv4 アドレスを割り当てます。この属性は、ローカルユーザビューでのみ設定可能です。ユーザグループビューでは設定できません。

ip-pool *ipv4-pool-name*: ユーザの IPv4 アドレスプールを指定します。*ipv4-pool-name* 引数は、大文字と小文字を区別しない 1 から 63 文字の文字列です。

primary-dns ip *ipv4-address*: ユーザのプライマリ DNS サーバの IPv 4 アドレスを指定します。

user-profile *profile-name*: 許可ユーザプロファイルを指定します。設定範囲は 1〜31 です。大文字、小文字を区別します。ユーザプロファイル名は英字、数字、アンダーライン（_）のみ使用することができます。ユーザプロファイルは認証されたユーザの動作を制限します。

user-role *role-name*: 許可されたユーザロールを指定します。設定範囲は 1〜63 です。大文字、小文字を区別します。ユーザに 64 のユーザロールを指定することができます。このオプションは local user view でのみ有効で、user group view では無効です。

vlan *vlan-id*: 許可 VLAN を指定します。設定範囲は 1〜4094 です。認証にパスし、VLAN が許可されたのち、ローカルユーザは VLAN のリソースのみアクセスすることができます。

session-timeout *minutes*: ユーザのセッションタイムアウトタイマを分単位で指定します。minutes 引数の値の範囲は 1 から 1440 です。タイマの期限が切れると、装置はユーザをログオフします。

url *url-string*: リダイレクト URL を指定します。url-string 引数は、1 から 255 文字の大文字と小文字を区別する文字列です。URL は http ://または https ://.で始まる必要があります。ユーザが認証を通過した後、または請求期限超過通知をユーザにプッシュした後、ユーザに広告または通知をプッシュするようにリダイレクト URL 属性を設定できます。このオプションは、LAN ユーザにのみ適用されます。

user-profile *profile-name*: 認可ユーザプロファイルを名前で指定します。profile-name 引数は、1 から 31 文字の大文字と小文字を区別する文字列です。ユーザプロファイル名には、文字、数字、ハイフン(-)、アンダーバー(_)のみを使用できます。文字または数字で始めることはできますが、すべて数字にすることはできません。ユーザプロファイルは、認証されたユーザの動作を制限します。

user-role *role-name*: 権限のあるユーザロールを指定します。role-name 引数は、1 から 63 文字の大文字と小文字を区別する文字列です。ユーザには最大 64 個のユーザロールを指定できます。ユーザロール関連のコマンドについては、RBAC コマンドの基本的なコマンドリファレンスを参照してください。このオプションはローカルユーザビューでのみ使用でき、ユーザグループビューでは使用できません。

vlan *vlan-id*: 許可された VLAN を指定します。vlan-id 引数の値の範囲は 1 から 4094 です。認証に成功し、VLAN が許可されると、ローカルユーザはこの VLAN 内のリソースにのみアクセスできます。

work-directory *directory-name*: FTP、SFTP ユーザの作業ディレクトリを指定します。設定範囲は 1〜255 です。大文字、小文字を区別しません。このディレクトリは既に存在している必要があります。デフォルトで FTP、SFTP ユーザは装置のルートディレクトリにアクセスすることができます。

説明

authorization-attribute コマンドはローカルユーザまたはユーザグループの許可属性を設定します。ローカルユーザ、またはローカルユーザのユーザグループが認証を通過すると、装置はユーザにそれらの属性を割り当てます。

undo authorization-attribute コマンドはデフォルトに戻します。

アプリケーション環境と目的に従って許可属性を設定してください。ユーザのサービスタイプに依存して許可属性をサポートします。

PPP ユーザの場合、callback-number、idle-cut、ip、ip-pool、primary-dns、secondary-dns、user-profile、および session-timeout の認可属性のみが有効になります。

ポータルユーザの場合、idle-cut、acl、ip-pool、user-profile、および session-timeout の認可属性のみが有効になります。

LAN ユーザの場合、acl、idle-cut、session-timeout、user-profile、ulr、および vlan の認可属性のみが有効になります。idle-cut 認可属性は、無線ユーザに対してのみ有効になります。

SSH、Telnet、およびターミナルユーザの場合、user-role authorization 属性のみが有効になります。

HTTP および HTTPS ユーザの場合、authorization 属性 user-role のみが有効になります。

FTP ユーザの場合、authorization 属性 user-role および work-directory のみが有効になります。

IKE ユーザの場合、authorization 属性 ip-pool のみが有効になります。

その他のタイプのローカルユーザの場合、authorization 属性は有効になりません。

ユーザグループに設定された認可属性は、グループ内のすべてのローカルユーザを対象としています。ローカルユーザをグループ化して、設定と管理の効率を向上させることができます。ローカルユーザビューで設定された認可属性は、ユーザグループビューで設定された同じ属性よりも優先されます。

認可 ACL を指定する場合、次の制限が適用されます。

- 認可 ACL が存在しない場合、または規則が含まれていない場合は無効です。この状況でポータルユーザに対して認可 ACL の厳密なチェックが有効になっている場合、ポータルユーザは強制的にオフラインになります。
- 認証を通過した後にポータルユーザがオンラインになるように、に割り当てられた ACL に送信元 IP または MAC アドレスで指定されたルールがないことを確認します。

このコマンドを使用して許可されたユーザロールのみをユーザが持つようにするには、undo authorization-attribute user-role コマンドを使用してデフォルトのユーザロールを削除します。

security-audit ユーザロールは、セキュリティログファイルおよびセキュリティログファイルシステムを管理するためのコマンドにアクセスできます。security-audit ユーザロールのアクセス可能なすべてのコマンドを表示するには、display role name security-audit コマンドを使用します。セキュリティログ管理の詳細については、コマンドマニュアルのセクション 1 *基本機能 “information center”* を参照してください。ファイルシステム管理の詳細については、コマンドマニュアルのセクション 1 *基本機能 “ファイルシステム管理”* を参照してください。

例

ネットワークアクセスユーザ abc の許可される VLAN を VLAN 2 として設定します。

<AP> system-view

[AP] local-user abc class network

[AP-luser-network-abc] authorization-attribute vlan 2

ユーザグループ abc の許可される VLAN を VLAN3 として設定します。

<AP> system-view

[AP] user-group abc

[AP-ugroup-abc] authorization-attribute vlan 3

セキュリティ監査ユーザロールを装置管理ユーザ xyz に権限ユーザロールとして割り当てます。

<AP>system-view

[AP]local-user xyz class manage

[AP-luser-manage-xyz]authorization-attribute user-role security-audit

```
This operation will delete all other roles of the user. Are you sure? [Y/N]:y
```

関連コマンド

- **display local-user**
- **display user-group**

3.2.3 bind-attribute

Syntax

bind-attribute { **call-number** call-number [: subcall-number] | **ip** ip-address | **location interface** interface-type interface-number | **mac** mac-address | **vlan** vlan-id } *

undo bind-attribute { **ip** | **location** | **mac** | **vlan** } *

デフォルト

設定なし

View

Local user view

定義済みユーザロール

network-admin

パラメータ

call-number *call-number*: PPP ユーザ認証の発信番号を指定します。call-number 引数は、1 から 64 文字の文字列です。このオプションは、PPP ユーザにのみ適用されます。

ip *ip-address*: ユーザの IP アドレスを指定します。このオプションは 802.1X ユーザのみ適用可能です。

location interface *interface-type interface-number*: ユーザのインタフェースを指定します。*interface-type* はインタフェースタイプ、*interface-number* はインタフェース番号を示します。認証にパスするため、ユーザはインタフェースを通してネットワークにアクセスする必要があります。このオプションは LAN ユーザのみ適用可能です。無線インタフェースに指定しないでください。

mac *mac-address*: ユーザの MAC アドレスを指定します。形式は H-H-H です。このオプションは LAN ユーザのみ適用可能です。

vlan *vlan-id*: ユーザが所属する VLAN を指定します。設定範囲は 1～4094 です。このオプションは LAN ユーザのみ適用可能です。

説明

bind-attribute コマンドはローカルユーザのバインディング属性を設定します。

undo bind-attribute コマンドはローカルユーザのバインディング属性を削除します。

ユーザのローカル認証を実行するため、装置はユーザの属性と設定されたバインディング属性を一致させます。ユーザが属性に一致しない、あるいは必要な属性が不足している場合、ユーザは認証に失敗します。

バインディング属性のチェックはすべてのアクセスサービスに適用します。

アクセスサービスにもとづいたユーザのバインディング属性を設定してください。装置はユーザのパケットから取得したすべての属性を確認します。たとえば、802.1X 認証は

パケット内のユーザの IP アドレスを含むため、802.1X ユーザの IP アドレスのバンディング属性を設定することができます。しかし MAC アドレス認証は IP アドレスを使用しないため、MAC アドレス認証ユーザの IP アドレスのバインディング属性を設定することはできません。

バインディングするインタフェースタイプはローカルユーザの要件に合わせる必要があります。ユーザのサービスタイプにもとづいてインタフェースの割り当てを設定してください。

- ユーザが 802.1X ユーザの場合、802.1X が有効なレイヤ 2 Ethernet インタフェースを指定してください。
- ユーザが MAC アドレス認証ユーザの場合、MAC アドレス認証が有効なレイヤ 2 Ethernet インタフェースを指定してください。
- ユーザがインタフェースユーザの場合は、ポータル対応ポータルを指定します。VLAN インタフェースでインタフェースが有効であり、portal roaming enable コマンドが設定されていない場合は、レイヤ 2 Ethernet ポータルを指定します。

例

ネットワークアクセスユーザ abc に IP アドレス 3.3.3.3 を割り当てます。

<AP> system-view

[AP] local-user abc class network

[AP-luser-network-abc] bind-attribute ip 3.3.3.3

関連コマンド

display local-user

3.2.4 description (network access user view)

Syntax

description *text*

undo description

デフォルト

設定なし

View

Network access user view

定義済みユーザロール

network-admin

パラメータ

text: ネットワークアクセスユーザの説明を指定します。大文字と小文字を区別する 1 から 127 文字の文字列です。

説明

description コマンドはネットワークアクセスユーザの説明を設定します。

undo description コマンドはデフォルトに戻します。

Web インタフェースで特別な表示または管理目的でネットワークアクセスユーザをマークするには、そのユーザの description #user_from_server#を設定します。目的は Web インタフェースの実装によって異なります。

例

ネットワークアクセスユーザ 123 の説明として Manager of MSC company を設定します。

<AP> system-view

[AP] local-user 123 class network

[AP-luser-network-123] description Manager of MSC company

関連コマンド

display local-user

3.2.5 display local-user

Syntax

display local-user [**class** { **manage** | **network** [**guest**] } | **idle-cut** { **disable** | **enable** } | **service-type** { **ftp** | **http** | **https** | **ike** | **lan-access** | **portal** | ppp | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name class* { **manage** | **network** [**guest**] } | **vlan** vlan-id]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

class: ローカルユーザタイプを指定します。

manage: 装置管理ユーザを指定します。
network: ネットワークアクセスユーザを指定します。

idle-cut { **disable** | **enable** }: アイドルカット機能が有効、または無効になっているローカルユーザを指定します。

service-type: サービスの指定タイプを使用するローカルユーザを指定します。

ftp: FTP ユーザを指定します。
http: HTTP ユーザを指定します。
lan-access: 802.1x ユーザなど、イーサネット経由でネットワークにアクセスするユーザを指定します。
portal: ポータルユーザ。
ppp: PPP ユーザ。
ssh: SSH ユーザを指定します。
telnet: Telnet ユーザを指定します。
terminal: コンソールポートを使用してログインする端末ユーザを指定します。

state { **active** | **block** }: アクティブまたはブロック状態にあるローカルユーザを指定します。アクティブ状態のローカルユーザは、ネットワークサービスにアクセスできます。ブロック状態のローカルユーザは認証、許可、アカウンティングサービスに要求することができません。

user-name *user-name*: 指定されたユーザ名を使用したすべてのローカルユーザを指定します。設定範囲は 1～55 です。大文字、小文字を区別します。

- ドメイン名を含めることはできません。
- スラッシュ（/），バックスラッシュ、垂直バー（|）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）を含めることはできません。（a）、（al）、（all）は使用できません。

- ドメイン名を含むユーザ名は、pure-username@domain-name 形式です。
  - ユーザ名部分は大文字と小文字が区別されます。スラッシュ（/），バックスラッシュ、垂直バー（|）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）を含めることはできません。（a）、（al）、（all）は使用できません
  - ドメイン名の部分は大文字と小文字を区別せず、アットマーク(@)を含めることはできません。

vlan *vlan-id*: VLAN のすべてのローカルユーザを指定します。設定範囲は 1～4094 です。

説明

display local-user コマンドはローカルユーザの設定、オンラインユーザの統計情報を表示します。

パラメータを指定しない場合、すべてのローカルユーザの情報を表示します。

例

すべてのローカルユーザの情報を表示します。

<AP> display local-user

```
Device management user root:
 State:                Active
 Service type:          SSH/Telnet/Terminal
 Access limit:          Enabled         Max access number: 3
 Current access number:   1
 User group:            system
 Bind attributes:
 Authorization attributes:
  Work directory:        flash:
  User role list:        network-admin
Network access user jj:
 State:                Active
 Service type:          Lan-access
 User group:            system
 Bind attributes:
  IP address:           2.2.2.2
  Location bound:        GigabitEthernet1/0/1
  MAC address:          0001-0001-0001
  VLAN ID:              2
  Calling number:        2:2
 Authorization attributes:
  Idle timeout:          33 minutes
  Work directory:        flash:
  ACL number:           2000
  User profile:          pp
```

```
  User role list:         network-operator, level-0, level-3
Network access guest user user1:
  State:                  Active
  Service type:            LAN access/Portal
  User group:              guest1
  Full name:               Jack
  Company:                 cc
  Email:                   Jack@cc.com
  Phone:                   131129237
  Description:             A guest from company cc
  Sponsor full name:        Sam
  Sponsor department:       security
  Sponsor email:           Sam@aa.com
  Period of validity::
    Start date and time:    2015/04/01-08:00:00
    Expiration date and time:2015/04/03-18:00:00
Total 3 local users matched.
```

表 3-2 コマンド出力

フィールド	説明
State	ローカルユーザの状態（アクティブまたはブロック）です。
Service Type	ローカルユーザが使用可能なサービスタイプです。
Access limit	同時にログインできる接続数を制限しているかどうかを示します。
Max access number	ローカルユーザ名を使用して同時にログインする最大接続数です。
Current access number	ローカルユーザ名を使用して同時にログインしている現在の接続数です。
User Group	ローカルユーザのグループです。
Bind attributes	ローカルユーザのバインディング属性です。
IP address	ローカルユーザのIPアドレスです。
Location bound	ローカルユーザのバインディングポートです。
MAC address	ローカルユーザのMACアドレスです。
VLAN ID	ローカルユーザのバインディングVLANです。
Calling number	ISDNユーザの発信者番号です。

フィールド	説明
Authorization attributes	ローカルユーザの許可属性です。
Idle timeout	ユーザのアイドルタイムアウト時間です。単位は分です。
Session-timeout	ユーザのセッションタイムアウト時間です。単位は分です。
Callback number	ローカルユーザの許可されたPPPコールバック番号です。
Work directory	ユーザがアクセスできるFTP、SFTPのディレクトリです。
ACL Number	ローカルユーザの許可ACLです。
VLAN ID	ローカルユーザの許可VLANです。
User profile	ローカルユーザの許可ユーザプロファイルです。
User role list	ローカルユーザの許可ロールです。
URL	ローカルユーザのリダイレクトURLです。
IP pool	ネットワークアクセスユーザの説明です。
Start date and time	ローカルユーザに許可されたIPv 4アドレスプールです。
IP address	ローカルユーザに許可されたIPv 4アドレスです。
Primary DNS server	ローカルユーザのプライマリDNSサーバのIPv4アドレスです。
Secondary DNS server	ローカルユーザのセカンダリDNSサーバのIPv4アドレスです。
URL	ローカルユーザのリダイレクトURLです。
Full name	ローカルゲストの名前です
Company	ローカルゲストの会社名です。
Email	ローカルゲストの電子メールアドレスです。
Phone	ローカルゲストの電話番号です。
Sponsor full name	ゲストスポンサーの名前です。
Sponsor department	ゲストスポンサーの部署です。
Sponsor email	ゲストスポンサーの電子メールアドレスです。

フィールド	説明
Description	ネットワークアクセスユーザの説明です。
Validity period	ネットワークアクセスユーザの有効期間です。
Start date and time	ネットワークアクセスユーザが適用された日時です。
Expiration date and time	ネットワークアクセスユーザの有効期限が終了する日時です。

3.2.6 display user-group

Syntax

display user-group { **all** | **name** *group-name* [**byod-authorization**] } [**identity-member** { **all** | **group** | **user** }]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

all: すべてのユーザグループを指定します。

name *group-name*: ユーザグループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

byod-authorization: BYOD 許可情報を指定します。このキーワードを指定しない場合、コマンドは BYOD 許可情報を表示せず、BYOD 許可属性が設定されているかどうかのみを表示します。

identity-member { **all** | **group** | **user** }: 指定したユーザグループまたはすべてのユーザグループの ID メンバーを指定します。このオプションを指定しない場合、コマンドは ID メンバー情報を表示しません。

- **all**: ID ユーザと ID グループを含むすべての ID メンバーを指定します。
- **group**: ID グループを指定します。
- **user**: ID ユーザを指定します。

説明

display user-group コマンドはユーザグループの設定を表示します。

例

すべてのユーザグループの設定を表示します。

<AP> display user-group all

```
Total 2 user groups matched.

User group: system
  Authorization attributes:
    Work directory:         flash:
User group: jj
  Authorization attributes:
  Idle timeout:           2 minutes
  Callback number:         2:2
  Work directory:          flash:/
  ACL number:             2000
  VLAN ID:                2
  User profile:            pp
```

すべてのユーザグループのすべての ID メンバーに関する情報を表示します。

<AP> display user-group all identity-member all

```
Total 2 user groups matched.

User group: system
Identity groups: 0
Identity users: 0
User group: jj
Description: school
Identity groups: 2
Group name                          Group description
1                                   group1
2                                   group2
Identity users: 2
User ID Username
0x234             user1
0xffffffff        user2
```

表 3-3 コマンド出力

フィールド	説明
User group	ユーザグループの名称です。
Authorization attributes	ユーザグループの許可属性です。
Idle timeout	アイドルタイムアウト時間です。単位は分です。

フィールド	説明
Session-timeout	セッションタイムアウト時間です。単位は分です。
Callback number	許可されたPPPコールバック番号です。
Work Directory	グループのユーザがアクセスできるFTP、SFTPのディレクトリです。
ACL Number	許可ACLです。
VLAN ID	許可VLANです。
User profile	許可ユーザプロファイルです。
IP pool	ユーザグループに許可されたIPv 4アドレスプールです。
Primary DNS server	ユーザグループに許可されているプライマリDNSサーバのIPv 4アドレスです。
Secondary DNS server	ユーザグループに許可されたセカンダリDNSサーバのIPv 4アドレスです。
URL	ユーザグループのリダイレクトURLです。
BYOD authorization attributes	ユーザグループのBYOD許可属性です。

3.2.7 group

Syntax

group *group-name*

undo group

デフォルト

ローカルユーザは定義済みユーザグループ system に所属しています。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

group-name: ユーザグループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

group コマンドはユーザグループにローカルユーザを割り当てます。

undo group コマンドはデフォルトに戻します。

例

ユーザグループ abc に装置管理ユーザ 111 を割り当てます。

<AP> system-view

[AP] local-user 111 class manage

[AP-luser-manage-111] group abc

関連コマンド

display local-user

3.2.8 local-user

Syntax

local-user *user-name* [**class** { **manage** | **network** [**guest**] }]

undo local-user { *user-name* **class** { **manage** | **network** [**guest**] } | **all** [**service-type** { **ftp** | **http** | **https** | **ike** | **lan-access** | **portal** | **ppp** | **ssh** | **telnet** | **terminal** } | **class** { **manage** | **network** [**guest**] }] }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*: ローカルユーザ名を指定します。設定範囲は 1～55 です。大文字、小文字を区別します。

- ドメイン名を含めることはできません。
- スラッシュ（/）, バックスラッシュ、垂直バー（|）、コロン（:）、アスタリスク（*）、クエスチョンマーク（?）、小なり記号（<）、大なり記号（>）、アットマーク（@）
- （a）、（al）、（all）は使用できません。

class: ローカルユーザタイプを指定します。指定しない場合、装置管理ユーザを指定します。

manage: 装置管理ユーザを指定します。装置管理ユーザは FTP、HTTP、Telnet、SSH、端末サービスを使用することができます。
network: ネットワークのリソースにアクセスするネットワークアクセスユーザを指定します。ネットワークアクセスユーザは LAN アクセスサービスを使用することができます。
guest: 特定の有効期間中にデバイスを介してネットワークリソースにアクセスできるゲストです。ゲストは LAN アクセスおよびポータルサービスを使用できます。

all: すべてのユーザを指定します。

service-type: サービスの指定タイプを使用するローカルユーザを指定します。

ftp: FTP ユーザを指定します。
http: HTTP ユーザを指定します。
https: HTTPS ユーザを指定します。
ike: IKE 拡張認証を介してネットワークにアクセスする IKE ユーザを指定します。
lan-access: 802.1X ユーザなど、イーサネット経由でネットワークにアクセスするユーザを指定します。

portal: ポータルユーザを指定します。
ssh: SSH ユーザを指定します。
telnet: Telnet ユーザを指定します。
terminal: コンソールポートを使用してログインする端末ユーザを指定します。

説明

local-user コマンドはローカルユーザを追加し、local user view に移行します。

undo local-user コマンドはローカルユーザを削除します。

ローカル認証では、ユーザ名とユーザタイプによってローカルユーザが一意に識別されます。ユーザ名は、ユーザが入力したユーザ名から解析された純粋なユーザ名と一致するために使用されます。ユーザタイプは、ユーザが使用できるサービスタイプを制限します。

例

装置管理ユーザ user1 を追加し、local user view に移行します。

<AP> system-view

[AP] local-user user1 class manage

[AP-luser-manage-user1]

ネットワークアクセスユーザ user2 を追加し、local user view に移行します。

<AP> system-view

[AP] local-user user2 class network

[AP-luser-network-user2]

ネットワークアクセスユーザ user 3 を追加し、local guest view に移行します。

<AP> system-view

[AP] local-user user3 class network

[AP-luser-network-user3]

関連コマンド

- **display local-user**
- **service-type (local user view)**

3.2.9 password (device management user view)

Syntax

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

undo password

デフォルト

ローカルユーザのパスワードは設定されていません。正しいユーザ名を入力し、属性の確認を行った後、認証にパスできます。

View

Device management user view

定義済みユーザロール

network-admin

パラメータ

hash: ハッシュパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

string: パスワードを指定します。大文字、小文字を区別します。

- 暗号テキストの設定範囲は 1～117 文字です。
- ハッシュテキストのパスワードは 1～110 文字です。
- プレーンテキストのパスワードは 1～63 文字です。

説明

password コマンドはローカルユーザのパスワードを設定します。

undo password コマンドはローカルユーザのパスワードを削除します。

パラメータを指定しない場合、インタラクティブモードに移行し、プレーンパスワードを設定するようにメッセージが表示されます。

パスワードが指定されていない装置管理ユーザは、正しいユーザ名を入力して属性のチェックに合格すると、認証にパスできます。セキュリティを強化するには、装置管理ユーザごとにパスワードを設定します。

グローバルパスワード制御を有効にすると、装置は装置管理ユーザのパスワードを次のように処理します。

- 履歴レコード内のすべてのパスワードはハッシュ形式で保存されます。
- ユーザが自身のパスワードをプレーンテキストで変更した場合、システムは現在のプレーンパスワードの入力をユーザに要求します。新しいパスワードは、履歴レコード内のすべてのパスワードおよび現在のパスワードと異なる必要があります。ま

た、新しいパスワードは、現在のパスワードと異なる 4 文字以上である必要があります。

- あるユーザが別のユーザのパスワードをプレーンテキストで変更した場合、新しいパスワードは、そのユーザの履歴レコード内のすべてのパスワードおよび現在のパスワードと異なる必要があります。
- ユーザが自身のパスワードを削除した場合、システムは現在のプレーンパスワードの入力を要求します。
- 上記の状況を除き、システムはユーザに現在のプレーンパスワードの入力を要求したり、新しいパスワードと履歴レコードのパスワードおよび現在のパスワードを比較したりしません。

例

装置管理ユーザ user1 のパスワード 123456TESTplat&!をプレーンテキストで設定します。

<AP> system-view

[AP] local-user user1 class manage

[AP-luser-manage-user1] password simple 123456TESTplat&!

装置管理ユーザ test のパスワードをインタラクティブモードで設定します。

<AP> system-view

[AP] local-user test class manage

[AP-luser-manage-test] password

```
Password:
Confirm :
```

関連コマンド

display local-user

3.2.10 password (network access user view)

Syntax

password [{ **cipher** | **simple** } *string*]

undo password

デフォルト

ローカルユーザのパスワードは設定されていません。正しいユーザ名を入力し、属性の確認を行った後、認証にパスできます。

View

Network access user view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号テキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

string: パスワードを指定します。大文字、小文字を区別します。

- 暗号テキストの設定範囲は 1～117 文字です。
- ハッシュテキストのパスワードは 1～110 文字です。
- プレーンテキストのパスワードは 1～63 文字です。

説明

password コマンドはローカルユーザのパスワードを設定します。

undo password コマンドはローカルユーザのパスワードを削除します。

セキュリティを強化するためのベストプラクティスとして、ネットワークアクセスユーザごとにパスワードを設定します。

例

装置管理ユーザ user1 のパスワード 123456TESTplat&!をプレーンテキストで設定します。

<AP> system-view

[AP] local-user user1 class manage

[AP-luser-manage-user1] password simple 123456TESTplat&!

関連コマンド

display local-user

3.2.11 service-type (local user view)

Syntax

service-type { **ftp** | **lan-access** | { **http** | **https** | **portal** | **ssh** | **telnet** | **terminal** } * }

undo service-type { **ftp** | **lan-access** | { **http** | **https** | **portal** | **ssh** | **telnet** | **terminal** } * }

デフォルト

ローカルユーザは許可されておらず、サービスを使用することができません。

View

Local user view

定義済みユーザロール

network-admin

パラメータ

ftp: ユーザが FTP サービスを使用することを許可します。許可されたディレクトリは **authorization-attribute work-directory** コマンドで変更することができます。

http: HTTP サービスを使用することを許可します。

https: HTTPS サービスを使用することを許可します。

lan-access: ユーザが LAN アクセスサービスを使用することを許可します。一般的にユーザは 802.1X ユーザのようなイーサネットユーザです。

portal: ユーザがポータル認証サービスを使用することを許可します。

ssh: ユーザが SSH サービスを使用することを許可します。

telnet: ユーザが Telnet サービスを使用することを許可します。

terminal: ユーザが端末サービスを使用し、コンソールポートからログインすることを許可します。

説明

service-type コマンドはローカルユーザが使用するサービスタイプを指定します。

undo service-type コマンドはローカルユーザが使用するサービスタイプを削除します。

複数のサービスタイプをユーザに割り当てることができます。

例

装置管理ユーザ user1 が Telnet、FTP サービスを使用することを許可します。

<AP> system-view

[AP] local-user user1 class manage

[AP-luser-manage-user1] service-type telnet

[AP-luser-manage-user1] service-type ftp

関連コマンド

display local-user

3.2.12 state (local user view)

Syntax

state { **active** | **block** }

undo state

デフォルト

active

View

Local user view

定義済みユーザロール

network-admin

パラメータ

active: 現在のローカルユーザをアクティブ状態にし、現在のローカルユーザがネットワークサービスを要求できるようにします。

block: 現在のローカルユーザをブロック状態にします。ブロックされたローカルユーザはネットワークサービスを要求できなくなります。

説明

state コマンドはローカルユーザの状態を設定します。

undo state コマンドはデフォルトに戻します。

例

装置管理ユーザ user1 をブロック状態にします。

<AP> system-view

[AP] local-user user1 class manage

[AP-luser-manage-user1] state block

関連コマンド

display local-user

3.2.13 user-group

Syntax

user-group *group-name*

undo user-group *group-name*

デフォルト

システム定義のユーザグループが存在します。グループ名は **system** です。

View

System view

定義済みユーザロール

network-admin

パラメータ

group-name: ユーザグループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

user-group コマンドはユーザグループを作成し、user group view に移行します。ユーザグループが既に存在する場合、その view に移行します。

undo user-group コマンドはユーザグループを削除します。

ユーザグループはローカルユーザのグループで構成され、ローカルユーザの属性を設定します。グループ内でローカルユーザのユーザ属性の一元管理を実装するために、ユーザグループでローカルユーザの属性を設定することができます。ローカルユーザが存在するユーザグループは削除できません。

システム定義のユーザグループ **system** の設定は変更できますが、ユーザグループは削除できません。

例

ユーザグループ abc を作成し、user group view に移行します。

<AP> system-view

[AP] user-group abc

[AP-ugroup-abc]

関連コマンド

display user-group

3.3 RADIUS設定コマンド

3.3.1 accounting-on enable

Syntax

accounting-on enable [**interval** *interval* | **send** *send-times*] *

undo accounting-on enable

デフォルト

無効

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

interval *interval*: accounting-on パケットを再送する間隔を設定します。設定範囲は 1～15 秒です。デフォルトは 3 秒です。

send *send-times*: accounting-on パケットを送信する試行回数を指定します。設定範囲は 1～255 です。デフォルトは 50 です。

説明

accounting-on enable コマンドは accounting-on 機能を有効にします。

undo accounting-on enable コマンドは accounting-on 機能を無効にします。

accounting-on 機能は装置を再起動したのち、RADIUS サーバに accounting-on パケットを自動で送信します。accounting-on パケットを受信すると RADIUS サーバは装置に対してログインできるようにすべてのオンラインユーザをログアウトします。

次回の装置の再起動時に **accounting-on enable** コマンドを適用させるため、**save** コマンドを実行してください。**save** コマンドの詳細はコマンドマニュアルのセクション 1 *基本機能 “コンフィグレーションファイル管理”* を参照してください。

accounting-on enable コマンドのパラメータはコマンドを設定したのち、すぐに適用されます。

例

RADIUS スキーム radius1 で accounting-on 機能を有効にします。accounting-on パケットを再送する間隔を 5 秒に設定し、accounting-on パケットを送信する試行回数を 15 回に設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] accounting-on enable interval 5 send 15

関連コマンド

display radius scheme

3.3.2 data-flow-format (RADIUS scheme view)

Syntax

data-flow-format { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } } *

undo data-flow-format { **data** | **packet** }

デフォルト

データフローの単位は **byte**、データパケットの単位は **one-packet** です。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

data: データフローの単位を指定します。

byte: データフローの単位をバイトで指定します。

giga-byte: データフローの単位をギガバイトで指定します。

kilo-byte: データフローの単位をキロバイトで指定します。

mega-byte: データフローの単位をメガバイトで指定します。

packet: データパケットの単位をバイトで指定します。

giga-packet: データパケットの単位をギガバイトで指定します。

kilo-packet: データパケットの単位をキロバイトで指定します。

mega-packet: データパケットの単位をメガバイトで指定します。

one-packet: データパケットの単位を 1 パケットで指定します。

説明

data-flow-format コマンドはトラフィックの統計情報を送信する際に使用するデータフロー、またはパケットの単位を指定します。

undo data-flow-format コマンドはデフォルトに戻します。

トラフィックの統計情報を送信する際に使用するデータフロー、またはパケットの単位は RADIUS アカウンティングサーバの設定と同一にしてください。そうでなければアカウンティングは正しく実行できません。

例

RADIUS スキーム radius1 でデータフローの単位をキロバイト、パケットの単位をキロパケットに設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] data-flow-format data kilo-byte packet kilo-packet

関連コマンド

display radius scheme

3.3.3 display radius scheme

Syntax

display radius scheme [*radius-scheme-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

radius-scheme-name: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。RADIUS スキーム名を指定しない場合、すべての RADIUS スキームの設定が表示されます。

説明

display radius scheme コマンドは RADIUS スキームの設定を表示します。

例

すべての RADIUS スキームの設定を表示します。

<AP> display radius scheme

```
Total 1 RADIUS schemes

------------------------------------------------------------------
RADIUS scheme name: radius1
  Index : 0
  Primary authentication server:
    IP   : 2.2.2.2                          Port: 1812
    State: Active
    Test profile: 132
      Probe username: test
      Probe interval: 60 minutes
  Primary accounting server:
    IP : 1.1.1.1                            Port: 1813
    State: Active
  Second authentication server:
    IP : 3.3.3.3                            Port: 1812
    State: Block
    Test profile: Not configured
  Second accounting server:
    IP : 3.3.3.3                            Port: 1813
    State: Block (Mandatory)

  Accounting-On function                  : Enabled
    retransmission times                  : 5
    retransmission interval(seconds)      : 2
  Timeout Interval(seconds)               : 3
  Retransmission Times                    : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)            : 5
  Realtime Accounting Interval(seconds)   : 22
  NAS IP Address                          : 1.1.1.1
  User Name Format                        : with-domain
  Data flow unit                          : Megabyte
  Packet unit                             : One
  Attribute 15 check-mode                 : Strict
  Attribute 25                            : CAR
  Attribute Remanent-Volume unit          : Mega
  RADIUS server version (vendor ID 2011)  : 1.0
  Attribute 31 MAC format                 : hh:hh:hh:hh:hh:hh
------------------------------------------------------------------
```

表 3-4 コマンド出力

フィールド	説明
Index	RADIUSスキームのインデックス番号です。
Primary authentication server	プライマリ認証サーバの情報です。
Primary accounting server	プライマリアカウンティングサーバの情報です。
Second authentication server	セカンダリ認証サーバの情報です。
Second accounting server	セカンダリアカウンティングサーバの情報です。
IP	サーバのIPアドレスです。 サーバが設定されていない場合、**Not configured**と表示されます。
Port	サーバのサービスポート番号です。ポート番号が指定されていない場合、デフォルトのポート番号が表示されます。
State	サーバの状態です。 • **Active**–サーバはアクティブ状態です。 • **Block**–サーバは自動でブロック状態に変更されました。 • **Block (Mandatory)**–サーバを手動でブロック状態に設定しました。
duration	サーバの現在のアクティブ状態の継続時間です。このフィールドは、サーバがアクティブ状態の場合にのみ表示されます。
Most recent blocked period	サーバがブロック状態のままだったときの最新のブロック開始時刻と終了時刻です。サーバがまだブロック状態のままの場合は、終了時刻にnowが表示されます。
Most recent state changes	サーバの最新の5つの状態変更です。
Test profile	RADIUSサーバのステータス検出で使用されるテストプロファイルです。
Probe username	RADIUSサーバのステータス検出で使用されるユーザ名です。
Probe interval	サーバのステータス検出間隔です。単位は分です。
Probe count	デバイスがRADIUSサーバの到達可能性を判断するために必要な連続プローブ間隔の数です。
Weight	RADIUSサーバの重み。
Accounting-On function	accounting-on機能が有効にされているかどうかを示します。
extended function	拡張アカウンティング機能が有効かどうかを示しています。

フィールド	説明
retransmission times	accounting-onパケット転送の試行回数です。
retransmission interval(seconds)	accounting-onパケットの再送間隔です。単位は秒です。
Timeout Interval(seconds)	RADIUSサーバ応答タイムアウト間隔です。単位は秒です。
Retransmission times	単一RADIUSサーバにRADIUSパケットを転送する最大試行回数です。
Retransmission Times for Accounting Update	アカウンティングの最大試行回数です。
Server Quiet Period(minutes)	サーバの停止間隔です。単位は分です。
NAS IP Address	送信するRADIUSパケットの送信元IPアドレスです。
User Name Format	RADIUSサーバに送信されたユーザ名の形式です。以下の値が含まれます。 ● **with-domain**–ドメイン名を含みます。 ● **without-domain**–ドメイン名が除外されています。 ● **keep-original**–受信されたユーザ名をそのままユーザ名として転送します。
Data flow unit	データフローの単位です。
Packet unit	データパケットの単位です。
Attribute 15 check-mode	RADIUSがSSH、FTP、端末ユーザのログインサービス属性をチェックする方式です。 ● **Strict**–SSH、FTP、端末サービスのログインサービスの属性の値がそれぞれ50、51、52に一致するかどうかを確認します。 ● **Loose**–SSH、FTP、端末サービスの標準ログインサービスの属性が0に一致するか確認します。
Attribute 25	RADIUS属性25の中断状態です。 ● **Standard**–CARパラメータとして中断しません。 ● **CAR**–CARパラメータとして中断します。
Attribute Remanent-Volume unit	RADIUS Remanent_Volume属性のデータ単位です。
RADIUS server version (vendor ID 2011)	Vendor IDが2011のRADIUSサーバのバージョンです。 ● 1.0. ● 1.1.

フィールド	説明
Server-load-sharing	RADIUSサーバのロードシェアリング機能のステータスです。 ● **Disabled**–無効です。装置は、サーバの役割 (プライマリまたはセカンダリ) とサーバの可用性に基づいて選択されたサーバにトラフィックを転送します。 ● **Enabled**–機能は有効です。デバイスは、ロードシェアリングのために使用可能なサーバ間でトラフィックを分散します。
Attribute 30 MAC format	RADIUS属性30のMACアドレス形式です。
Attribute 31 MAC format	RADIUS属性31のMACアドレス形式です。
Attribute 182 vendor-ID 25506 VLAN	装置がMicrosegment-Id属性 (Vendor ID 25506の属性182) を許可VLANに認識できるようにするかどうか。
Parsing rules for attribute 18	応答メッセージ属性値が条件に一致した場合にユーザが実行するアクションです。 ● **New password**—新しいパスワードを入力します。 ● **Next toke**n—二要素認証の次の認証要素を入力します。
If match	装置がRADIUS Reply-Message属性を解析するためのルールです。
Action	一致基準です。二重引用符("")で囲まれた文字列です。

3.3.4 display radius statistics

Syntax

display radius statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display radius statistics コマンドは RADIUS パケットの統計情報を表示します。

例

RADIUS パケットの統計情報を表示します。

<AP> display radius statistics

```
                        Auth.        Acct.      SessCtrl.
        Request Packet:     0            0            0
          Retry Packet:     0            0            -
        Timeout Packet:     0            0            -
      Access Challenge:     0            -            -
        Account Start:      -            0            -
       Account Update:      -            0            -
         Account Stop:      -            0            -
    Terminate Request:      -            -            0
          Set Policy:       -            -            0
  Packet With Response:     0            0            0
Packet Without Response:    0            0            -
       Access Rejects:      0            -            -
       Dropped Packet:      0            0            0
       Check Failures:      0            0            0
```

表 3-5 コマンド出力

フィールド	説明
Auth.	認証パケットです。
Acct.	アカウンティングパケットです。

フィールド	説明
SessCtrl.	セッションコントロールパケットです。
Request Packet	パケット要求数です。
Retry Packet	パケット要求が再送された数です。
Timeout Packet	パケット要求がタイムアウトした数です。
Access Challenge	アクセスチャレンジを行ったパケット数です。
Account Start	スタートアカウンティング要求のパケット数です。
Account Update	アップデートアカウンティング要求のパケット数です。
Account Stop	ストップアカウンティング要求のパケット数です。
Terminate Request	強制的にユーザをログオフするためのパケット数です。
Set Policy	ユーザ許可情報をアップデートするパケット数です。
Packet With Response	応答が受信されたパケット数です。
Packet Without Response	応答が受信されていないパケット数です。
Access Rejects	アクセス拒否のパケット数です。
Dropped Packet	廃棄されたパケット数です。
Check Failures	チェックサムエラーのパケット数です。

関連コマンド

reset radius statistics

3.3.5 key (RADIUS scheme view)

Syntax

key { **accounting** | **authentication** } { **cipher** | **simple** } *string*

undo key { **accounting** | **authentication** }

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: セキュアな RADIUS アカウンティングの通信を行うために共有キーを設定します。

authentication: セキュアな RADIUS 認証の通信を行うために共有キーを設定します。

cipher: 暗号テキストの共有キーを設定します。

simple: プレーンテキストの共有キーを設定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。

- 暗号テキストの設定範囲は 1～117 文字です。
- プレーンテキストのパスワードは 1～64 文字です。

説明

key コマンドはセキュリティの高いセキュアな RADIUS 認証、アカウンティング通信を行うために共有キーを設定します。

undo key コマンドはセキュリティの高い RADIUS 認証、アカウンティング通信を行うための共有キーを削除します。

デフォルトに戻します。

このコマンドを使用して設定された共有キーはスキームのすべてのサーバに適用されます。

RADIUS サーバで設定された共有キーと一致していることを確認してください。

指定した RADIUS サーバの共有キーは **key** コマンドで指定された共有キーよりも優先されます。

例

RADIUS スキーム radius1 の共有キーok をプレーンテキストで設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] key accounting simple ok

関連コマンド

display radius scheme

3.3.6 nas-ip (RADIUS scheme view)

Syntax

nas-ip *ipv4-address*

undo nas-ip

デフォルト

サーバへ送信されるパケットの送信元 IP アドレスは、system view の **radius nas-ip** コマンドを使用して指定されます。

radius nas-ip コマンドが設定されていない場合、送信元インタフェースのプライマリ IP アドレスがパケットの送信元 IP アドレスとなります。

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: 装置の IPv4 アドレスを指定します。0.0.0.0、255.255.255.255、クラス D アドレス、クラス E アドレス、ループバックアドレスを指定することはできません。

説明

nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを設定します。

undo nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを削除します。

NAS が送信した RADIUS パケットの送信元 IP アドレスは RADIUS サーバに設定されている NAS の IP アドレスと一致する必要があります。RADIUS サーバは IP アドレスで NAS を識別します。RADIUS パケットを受信すると、RADIUS サーバは、パケットの送信元 IP アドレスが任意の管理 NAS の IP アドレスであるかどうかチェックします。

- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致する場合、サーバはパケットを処理します。
- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致しない場合、サーバはパケットを廃棄します。

サーバへ送信される RADIUS パケットの送信元アドレスとしてループバックインタフェースの IP アドレスを設定することを推奨します。

nas-ip コマンドと **radius nas-ip** コマンドの両方を使用する場合、以下のガイドラインに従います。

- RADIUS scheme view の **nas-ip** コマンドは、現在の RADIUS スキームにのみ適用されます。

- system view の **radius nas-ip** コマンドは、すべての RADIUS スキームに適用されます。
- RADIUS scheme view の **nas-ip** コマンドで設定されたコマンドは system view の **radius nas-ip** コマンドで設定されたコマンドよりも優先されます。

RADIUS スキームは、発信 RADIUS パケット用に送信元 IPv4 アドレスを 1 つだけ設定することができます。同じ RADIUS スキーム用に新しい送信元 IP アドレスを指定する場合、最後に指定されたコマンドが適用されます。

例

RADIUS スキーム radius1 でサーバへ送信される RADIUS パケットの送信元アドレス 10.1.1.1 を設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] nas-ip 10.1.1.1

関連コマンド

- **display radius scheme**
- **radius nas-ip**

3.3.7 primary accounting (RADIUS scheme view)

Syntax

primary accounting *ipv4-address* [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

undo primary accounting

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: プライマリ RADIUS アカウンティングサーバの IPv4 アドレスを指定します。

port-number: プライマリ RADIUS アカウンティングサーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1〜65535 です。デフォルトは 1813 です。

key: セキュアなプライマリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1〜117 文字です。プレーンテキストの設定範囲は 1〜64 文字です。

weight *weight-value*: 重み付けロードバランシングのための RADIUS サーバの重みを指定します。weight-value 引数の値の範囲は 0〜100 で、デフォルト値は 0 です。サーバの重みは、RADIUS スキームに対して RADIUS サーバのロードバランシングが有効になっている場合に有効になります。要求処理にサーバを使用しない場合は、その重みを 0 に設定します。より多くの要求をサーバに分散するには、そのサーバに高い重みを割り当てます。

説明

primary accounting コマンドはプライマリ RADIUS アカウンティングサーバを指定します。

undo primary accounting コマンドはプライマリ RADIUS アカウンティングサーバの設定を削除します。

プライマリ RADIUS アカウンティングサーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

スキームのプライマリとセカンダリの 2 つのアカウンティングサーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

primary accounting コマンドで設定された共有キーは **key accounting** コマンドで設定された共有キーよりも優先されます。

装置がアカウンティング開始要求を送信している間に、アカウンティングサーバを変更または削除すると、そのサーバとの通信がタイムアウトします。タイムアウト時にデバイスが実行するアクションは、RADIUS スキームの RADIUS サーバロードシェアリングの有効化ステータスによって異なります。

- RADIUS サーバのロードシェアリングが無効になっている場合、装置は、アカウンティングの優先順位が最も高いアクティブサーバとの通信を試みます。
- RADIUS サーバのロードシェアリングが有効になっている場合、装置は別のアクティブなアカウンティングサーバを検索するのではなく、アカウンティング失敗メッセージを返します。

もしアクティブな使用されているアカウンティングサーバを削除する場合、装置はユーザのリアルタイムアカウンティング要求とストップアカウンティング要求を送信しません。ストップアカウンティング要求を保持することはできません。装置は不正確なアカウンティングの結果を生成する可能性があります。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.2、UDP ポート番号 1813、プレーンテキスト共有キー123456TESTacct&!のプライマリアカウンティングサーバを指定します。

```
<AP> system-view
[AP] radius scheme radius1
[AP-radius-radius1] primary accounting 10.110.1.2 1813 key simple 123456TESTacct&!
```

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **secondary accounting (RADIUS scheme view)**

3.3.8 primary authentication (RADIUS scheme view)

Syntax

primary authentication *ipv4-address* [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

undo primary authentication

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: プライマリ RADIUS 認証サーバの IPv4 アドレスを指定します。

port-number: プライマリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: セキュアなプライマリ RADIUS サーバとのセキュア通信のための共有キーを指定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

test-profile *profile-name*：RADIUS サーバの状態を検出するためのテストプロファイルを指定します。大文字と小文字を区別する 1 から 31 文字の文字列です。

weight *weight-value*: 重み付けロードバランシングのための RADIUS サーバの重みを指定します。weight-value 引数の値の範囲は 0～100 で、デフォルト値は 0 です。サーバの重みは、RADIUS スキームに対して RADIUS サーバのロードバランシングが有効になっている場合に有効になります。要求処理にサーバを使用しない場合は、その重みを 0 に設定します。より多くの要求をサーバに分散するには、そのサーバに高い重みを割り当てます。

説明

primary authentication コマンドはプライマリ RADIUS 認証サーバを指定します。

undo primary authentication コマンドはプライマリ RADIUS 認証サーバの設定を削除します。

プライマリ RADIUS 認証サーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

スキームのプライマリとセカンダリの 2 つの認証サーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

primary authentication コマンドで設定された共有キーは **key authentication** コマンドで設定された共有キーよりも優先されます。

テストプロファイルが指定されている場合、装置は RADIUS サーバが利用可能か検出を行います。

primary authentication コマンドを使用して認証の処理中にプライマリ認証サーバを修正あるいは削除する場合、プライマリサーバとの通信はタイムアウトします。

装置は認証を行うため、もっとも高い優先度のアクティブなサーバと通信をしようとします。

装置がアカウンティング開始要求を送信している間に、アカウンティングサーバを変更または削除すると、そのサーバとの通信がタイムアウトします。タイムアウト時にデバイスが実行するアクションは、RADIUS スキームの RADIUS サーバロードシェアリングの有効化ステータスによって異なります。

- RADIUS サーバのロードシェアリングが無効になっている場合、装置は、アカウンティングの優先順位が最も高いアクティブサーバとの通信を試みます。
- RADIUS サーバのロードシェアリングが有効になっている場合、デバイスは重みと負荷に基づいてすべてのアクティブな認証サーバからサーバを再選択し、そのサーバに要求を送信します。

認証プロセス中にプライマリ認証サーバを変更または削除すると、プライマリサーバとの通信がタイムアウトします。デバイスは、認証の優先順位が最も高いアクティブサーバとの通信を試みます。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.1、UDP ポート番号 1812、プレーンテキスト共有キー123456TESTauth&!のプライマリ認証サーバを指定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] primary authentication 10.110.1.1 1812 key simple 123456TESTauth&!

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **radius-server test-profile**
- **secondary authentication (RADIUS scheme view)**

3.3.9 radius dscp

Syntax

radius dscp *dscp-value*

undo radius dscp

デフォルト

0

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: RADIUS パケットの DSCP 値を指定します。設定範囲は 0〜63 です。値が大きいほど、優先度は高くなります。

説明

radius dscp コマンドは RADIUS パケットの DSCP 値を設定します。

undo radius dscp コマンドはデフォルトに戻します。

RADIUS パケットの優先度を変更するため、ToS フィールドの DSCP 値を設定します。

例

IPv4 RADIUS パケットの DSCP 値を 10 に設定します。

<AP> system-view

[AP] radius dscp 10

3.3.10 radius nas-ip

Syntax

radius nas-ip *ipv4-address*

undo radius nas-ip *ipv4-address*

デフォルト

サーバへ送信されるパケットの送信元 IP アドレスは、送信元インタフェースの IP アドレスがパケットの送信元 IP アドレスとなります。

View

System view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: 装置の IPv4 アドレスを指定します。0.0.0.0、255.255.255.255、クラス D アドレス、クラス E アドレス、ループバックアドレスを指定することはできません。

説明

radius nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを設定します。

undo radius nas-ip コマンドはサーバへ送信される RADIUS パケットの送信元アドレスを削除します。

NAS が送信した RADIUS パケットの送信元 IP アドレスは RADIUS サーバに設定されている NAS の IP アドレスと一致する必要があります。RADIUS サーバは IP アドレスで NAS を識別します。RADIUS パケットを受信すると、RADIUS サーバは、パケットの送信元 IP アドレスが任意の管理 NAS の IP アドレスであるかどうかチェックします。

- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致する場合、サーバはパケットを処理します。
- パケットの送信元 IP アドレスが管理 NAS の IP アドレスと一致しない場合、サーバはパケットを廃棄します。

サーバへ送信される RADIUS パケットの送信元アドレスが指定されていない場合、サーバから戻ったパケットは物理ポートエラーとして装置に到着することができません。

nas-ip コマンドと **radius nas-ip** コマンドの両方を使用する場合、以下のガイドラインに従います。

- RADIUS scheme view の **nas-ip** コマンドは、現在の RADIUS スキームにのみ適用されます。
- system view の **radius nas-ip** コマンドは、すべての RADIUS スキームに適用されます。

- RADIUS scheme view の **nas-ip** コマンドで設定されたコマンドは system view の **radius nas-ip** コマンドで設定されたコマンドよりも優先されます。

新しい送信元 IPv4 アドレスを指定する場合、最後に指定されたコマンドが適用されます。

例

サーバへ送信される RADIUS パケットの送信元アドレス 129.10.10.1 を設定します。

<AP> system-view

[AP] radius nas-ip 129.10.10.1

関連コマンド

nas-ip (RADIUS scheme view)

3.3.11 radius scheme

Syntax

radius scheme *radius-scheme-name*

undo radius scheme *radius-scheme-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

radius-scheme-name: RADIUS スキーム名を指定します。設定範囲は 1～32 です。大文字、小文字を区別しません。

説明

radius scheme コマンドは RADIUS スキームを作成し、RADIUS scheme view に移行します。

undo radius scheme コマンドは RADIUS スキームを削除します。

RADIUS スキームは、同時に 2 つ以上の ISP ドメインで使用されることがあります。

装置は最大 16 までの RADIUS スキームをサポートしています。

例

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1]

関連コマンド

display radius scheme

3.3.12 radius-server test-profile

Syntax

radius-server test-profile *profile-name* **username** *name* [**interval** *interval*]

undo radius-server test-profile *profile-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: テストプロファイルの名前を指定します。大文字と小文字を区別します。文字数は 1～31 文字です。

username *name*: 検出パケット内のユーザ名を指定します。*name* パラメータは大文字と小文字を区別し、1～253 文字で指定します。

interval *interval*: 検出パケットを送信する間隔を分で設定します。*Interval* パラメータの値の範囲は 1～3600 で、デフォルトは 60 です。

説明

radius-server test-profile コマンドは RADIUS サーバの状態を検出するためのテストプロファイルを設定します。

undo radius-server test-profile コマンドはテストプロファイルを削除します。

装置は、サーバに対して指定されたテストプロファイルが存在する場合にのみ、RADIUS サーバの状態検出を開始します。存在しないテストプロファイルを RADIUS サーバに対して指定した場合、装置上にテストプロファイルを作成するまで、装置はサーバの状態を検出しません。

テストプロファイルを削除すると、装置は削除したテストプロファイルを使用していた RADIUS サーバの状態の検出を停止します。

このコマンドを複数回実行することで、複数のテストプロファイルを設定できます。

例

RADIUS サーバの状態を検出するためにテストプロファイル **abc** を設定します。ユーザ名 **admin** を使用した検出パケットを 10 分ごとに送信します。

<AP> system-view

[AP] radius-server test-profile abc username admin interval 10

関連コマンド

primary authentication（コマンドマニュアルのセクション 12 *ユーザアクセスと認証 “AAA”*）

secondary authentication（コマンドマニュアルのセクション 12 *ユーザアクセスと認証 “AAA”*）

3.3.13 reset radius statistics

Syntax

reset radius statistics

View

User view

定義済みユーザロール

network-admin

説明

reset radius statistics コマンドは RADIUS 統計情報を削除します。

例

RADIUS 統計情報を削除します。

<AP> reset radius statistics

関連コマンド

display radius statistics

3.3.14 retry

Syntax

retry *retries*

undo retry

デフォルト

3

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries: RADIUS パケットの再送信の最大試行回数を設定します。設定範囲は 1～20 です。

説明

retry コマンドは 1 つの RADIUS サーバに再送 RADIUS パケットを送信する最大試行回数を設定します。

undo retry コマンドはデフォルトに戻します。

RADIUS はデータ送信に UDP パケットを使用しているため、通信に信頼性がありません。

装置が応答タイムアウト時間以内に RADIUS サーバから要求に対する応答を受信しない場合、装置は RADIUS 要求を再送します。タイムアウト時間を設定する場合、**timer response-timeout** コマンドを使用します。

再送の試行回数が上限に達しても、RADIUS サーバから応答がない場合、装置は要求が失敗したとみなします。

クライアントが認証プロセスの間にタイムアウトした場合、ユーザはすぐにログオフします。ユーザのログオフを防ぐため、以下によって乗算した値は、アクセスモジュールによって定義したクライアントのタイムアウト時間よりも大きくすることができません。

- RADIUS パケットの最大試行回数
- RADIUS サーバ応答タイムアウト時間
- RADIUS スキームの RADIUS 認証サーバ数

装置が新しい RADIUS サーバに RADIUS 要求を送信するとき、RADIUS パケットを転送する総時間を確認してください。総時間が 300 秒を超過した場合、次の RADIUS サーバへの RADIUS 要求の送信を停止します。

パケットの再送試行回数と RADIUS サーバの応答タイムアウト時間を設定する際に、RADIUS サーバの数を考慮してください。

例

RADIUS スキーム radius1 の再送 RADIUS パケットの最大試行回数を 5 に設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] retry 5

関連コマンド

- **radius scheme**
- **timer response-timeout (RADIUS scheme view)**

3.3.15 retry realtime-accounting

Syntax

retry realtime-accounting *retries*

undo retry realtime-accounting

デフォルト

5

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

retries: アカウンティング要求の再送信の最大試行回数を設定します。設定範囲は 1～255 です。

説明

retry realtime-accounting コマンドはアカウンティング要求を再送信する最大試行回数を設定します。

undo retry realtime-accounting コマンドはデフォルトに戻します。

通常、RADIUS アカウンティングサーバはタイムアウトタイマを使用して、ユーザがオンラインかどうかを確認します。タイムアウト時間内にサーバがリアルタイムアカウンティング要求を受信しない場合、回線または装置に不具合があるとみなします。サーバはユーザのアカウンティングを停止します。

この状況は、予期しない不具合が生じた場合に起こります。この場合、NAS は、アカウンティング要求の再送の最大試行回数に応じて、ユーザを適宜に切断するよう要求されます。最大回数に達しても応答がない場合、NAS は、ユーザを切断します。

たとえば、以下の条件があると仮定します。

- RADIUS サーバの応答タイムアウト時間が 3 秒とします。(**timer response-timeout** コマンドで設定します)
- RADIUS パケットの再送試行回数が 3 回とします。(**retry** コマンドで設定します)
- リアルタイムアカウンティング間隔が 12 分とします。(**timer realtime-accounting** コマンドで設定します。)
- アカウンティング要求を送信する最大試行回数が 5 回(**retry realtime-accounting** コマンドで設定します。)とします。

装置は 12 分ごとにアカウンティング要求を生成し、3 秒以内に応答がなければ、要求を再送します。3 回要求を送信する間に応答がなければアカウンティングは失敗とみなし、

別のアカウンティングを試行します。5 回連続してアカウンティングの送信が失敗した場合、装置はユーザ接続を切断します。

例

RADIUS スキーム radius1 のアカウンティング要求を送信する最大試行回数を 10 に設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] retry realtime-accounting 10

関連コマンド

- **retry**
- **timer realtime-accounting (RADIUS scheme view)**
- **timer response-timeout (RADIUS scheme view)**

3.3.16 secondary accounting (RADIUS scheme view)

Syntax

secondary accounting { *ipv4-address* } [*port-number* | **key** { **cipher** | **simple** } *string* | **weight** *weight-value*] *

undo secondary accounting [{ *ipv4-address* } [*port-number*]]

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: セカンダリ RADIUS アカウンティングサーバの IPv4 アドレスを指定します。

port-number: セカンダリ RADIUS アカウンティングサーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1〜65535 です。デフォルトは 1813 です。

key: セキュアなセカンダリ RADIUS アカウンティングサーバの通信を行うために共有キーを設定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1〜117 文字です。プレーンテキストの設定範囲は 1〜64 文字です。

weight *weight-value*: 重み付けロードバランシングのための RADIUS サーバの重みを指定します。weight-value 引数の値の範囲は 0〜100 で、デフォルト値は 0 です。サーバの重みは、RADIUS スキームに対して RADIUS サーバのロードバランシングが有効になっている場合に有効になります。要求処理にサーバを使用しない場合は、重みを 0 に設定します。より多くの要求をサーバに分散するには、そのサーバに高い重みを割り当てます。

説明

secondary accounting コマンドはセカンダリ RADIUS アカウンティングサーバを指定します。

undo secondary accounting コマンドはセカンダリ RADIUS アカウンティングサーバを削除します。

セカンダリ RADIUS アカウンティングサーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

RADIUS スキームに最大 16 のセカンダリ RADIUS アカウンティングサーバを設定することができます。プライマリサーバが故障したとき、装置はアクティブ状態のセカンダリサーバと通信しようとします。装置は設定された順番でセカンダリサーバと接続します。

スキームのプライマリとセカンダリの 2 つのアカウンティングサーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

secondary accounting コマンドで設定された共有キーは **key accounting** コマンドで設定された共有キーよりも優先されます。

secondary accounting コマンドを使用してスタートアカウンティング要求を送信するセカンダリアカウンティングサーバを修正あるいは削除する場合、セカンダリサーバとの通信はタイムアウトします。

装置がアカウンティング開始要求を送信している間に、アカウンティングサーバを変更または削除すると、そのサーバとの通信がタイムアウトします。タイムアウト時にデバイスが実行するアクションは、RADIUS スキームの RADIUS サーバロードシェアリングの有効化ステータスによって異なります。

- RADIUS サーバのロードシェアリングが無効になっている場合、デバイスは、アカウンティングの優先順位が最も高いアクティブサーバとの通信を試みます。
- RADIUS サーバのロードシェアリングが有効になっている場合、デバイスは別のアクティブなアカウンティングサーバを検索するのではなく、アカウンティング失敗メッセージを返します。

アクティブに使用されているアカウンティングサーバを削除すると、装置はユーザのリアルタイムアカウンティング要求と停止アカウンティング要求を送信しなくなります。また、装置は停止アカウンティング要求をバッファしません。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.1、UDP ポート番号 1813 のセカンダリアカウンティングサーバを指定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] secondary accounting 10.110.1.1 1813

RADIUS スキーム radius2 の 2 つのセカンダリアカウンティングサーバの IP アドレスを 10.110.1.1 と 10.110.1.2、UDP ポートを 1813 に指定します。

<AP> system-view

[AP] radius scheme radius2

[AP-radius-radius2] secondary accounting 10.110.1.1 1813

[AP-radius-radius2] secondary accounting 10.110.1.2 1813

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **primary accounting (RADIUS scheme view)**

3.3.17 secondary authentication (RADIUS scheme view)

Syntax

secondary authentication *ipv4-address* [*port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **weight** *weight-value*] *

undo secondary authentication [**ipv4-address** [*port-number*]]

デフォルト

設定なし

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: セカンダリ RADIUS 認証サーバの IPv4 アドレスを指定します。

port-number: セカンダリ RADIUS 認証サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。デフォルトは 1812 です。

key: プライマリ RADIUS 認証サーバとのセキュア通信のための共有キーを指定します。

cipher: 暗号テキストを指定します。

simple: プレーンテキストを指定します。セキュリティのため、プレーンテキストで設定された共有キーを含めたすべての共有キーは、暗号化されて保存されます。

string: 共有キーを指定します。大文字、小文字を区別します。暗号テキストの設定範囲は 1～117 文字です。プレーンテキストの設定範囲は 1～64 文字です。

test-profile *profile-name*：RADIUS サーバの状態を検出するためのテストプロファイルを指定します。大文字と小文字を区別する 1 から 31 文字の文字列です。

weight *weight-value*: 重み付けロードバランシングのための RADIUS サーバの重みを指定します。weight-value 引数の値の範囲は 0～100 で、デフォルト値は 0 です。サーバの重みは、RADIUS スキームに対して RADIUS サーバのロードバランシングが有効になっている場合に有効になります。要求処理にサーバを使用しない場合は、重みを 0 に設定します。より多くの要求をサーバに分散するには、そのサーバに高い重みを割り当てます。

説明

secondary authentication コマンドはセカンダリ RADIUS 認証サーバを指定します。

undo secondary authentication コマンドはセカンダリ RADIUS 認証サーバの設定を削除します。

セカンダリ RADIUS 認証サーバのポート番号と共有キーの設定は、サーバで設定された値と同一にしてください。

RADIUS スキームに最大 16 のセカンダリ RADIUS 認証サーバを設定することができます。プライマリサーバが故障したとき、装置はアクティブ状態のセカンダリサーバと通信しようとします。装置は設定された順番でセカンダリサーバと接続します。

指定されたテストプロファイルがデバイス上に存在する場合、サーバのステータス検出がトリガされます。

スキームのプライマリとセカンダリの 2 つの認証サーバでホスト名、IP アドレス、ポート番号を同一にすることはできません。

secondary authentication コマンドで設定された共有キーは **key authentication** コマンドで設定された共有キーよりも優先されます。

リクエストの認証処理中に認証サーバを変更または削除すると、サーバとの通信がタイムアウトします。タイムアウト時にデバイスが実行するアクションは、RADIUS スキームの RADIUS サーバロードシェアリングの有効化ステータスによって異なります。

- RADIUS サーバのロードシェアリングが無効になっている場合、デバイスは認証の優先順位が最も高いアクティブサーバとの通信を試みます。
- RADIUS サーバのロードシェアリングが有効になっている場合、デバイスはすべてのアクティブ認証サーバから重みと負荷に基づいてサーバを再選択し、そのサーバに要求を送信します。

例

RADIUS スキーム radius1 に IP アドレス 10.110.1.2、UDP ポート番号 1812 のセカンダリ認証サーバを指定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] secondary authentication 10.110.1.2 1812

RADIUS スキーム radius2 の 2 つのセカンダリ認証サーバの IP アドレスを 10.110.1.1 と 10.110.1.2、UDP ポートを 1812 に指定します。

<AP> system-view

[AP] radius scheme radius2

[AP-radius-radius2] secondary authentication 10.110.1.1 1812

[AP-radius-radius2] secondary authentication 10.110.1.2 1812

関連コマンド

- **display radius scheme**
- **key (RADIUS scheme view)**
- **radius-server test-profile**
- **primary authentication (RADIUS scheme view)**

3.3.18 state primary

Syntax

state primary { **accounting** | **authentication** } { **active** | **block** }

デフォルト

active

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: プライマリ RADIUS アカウンティングサーバの状態を設定します。

authentication: プライマリ RADIUS 認証サーバの状態を設定します。

active: RADIUS サーバの状態を **active**（正常稼動の状態）に設定します。

block: RADIUS サーバの状態を **block**（サービス外の状態）に設定します。

説明

state primary コマンドはプライマリ RADIUS サーバの状態を設定します。

プライマリサーバがアクティブ状態であるとき、装置は最初にプライマリサーバと通信しようとします。プライマリサーバが使用できない場合、以下の処理を行います。

- プライマリサーバの状態をブロックに変更します。
- サーバの停止タイマを開始します。
- アクティブ状態のセカンダリサーバと通信します。

プライマリサーバの停止タイマがタイムアウトすると、サーバの状態が自動的にアクティブに変化します。停止タイマがタイムアウトする前にサーバの状態をブロックに設定した場合、手動でアクティブ状態に設定しない限り、サーバが自動的にアクティブ状態に戻ることはありません。

プライマリサーバとすべてのセカンダリサーバがブロック状態であるとき、装置はプライマリサーバと通信しようとします。

- プライマリサーバが自動的にブロック状態になった場合、装置はプライマリサーバとの通信だけを試行します。
- プライマリサーバが手動でブロック状態になった場合、装置は設定された順序で自動的にブロック状態になったセカンダリサーバとの通信を試行します。

このコマンドは、プライマリ RADIUS 認証サーバに有効なテストプロファイルが指定されている場合に、RADIUS サーバのステータス検出機能に影響を与える可能性があります。

- サーバのステータスをブロックに設定すると、装置はサーバのステータスの検出を停止します。
- サーバのステータスをアクティブに設定すると、装置はサーバのステータスの検出を開始します。

例

RADIUS スキーム radius1 のプライマリ認証サーバの状態を block に設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] state primary authentication block

関連コマンド

- **display radius scheme**
- **state secondary**

3.3.19 state secondary

Syntax

state secondary { **accounting** | **authentication** } [*ipv4-address* [*port-number*]] { **active** | **block** }

デフォルト

active

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

accounting: セカンダリ RADIUS アカウンティングサーバの状態を設定します。

authentication: セカンダリ RADIUS 認証サーバの状態を設定します。

ipv4-address: セカンダリ RADIUS サーバの IPv4 アドレスを指定します。

port-number: セカンダリ RADIUS サーバのサービスポート番号を UDP ポート番号で指定します。設定範囲は 1～65535 です。セカンダリ RADIUS 認証サーバのデフォルトは 1812 です。セカンダリ RADIUS アカウンティングサーバのデフォルトは 1813 です。

active: RADIUS サーバの状態を **active**（正常稼動の状態）に設定します。

block: RADIUS サーバの状態を **block**（サービス外の状態）に設定します。

説明

state secondary コマンドはセカンダリ RADIUS サーバの状態を設定します。

IP アドレスが設定されていない場合、このコマンドはすべてのセカンダリサーバの状態を変更します。

装置がアクティブ状態のセカンダリサーバと通信できないことを知った場合、以下の処理を行います。

- 装置はセカンダリサーバの状態をブロックに変更します。
- サーバの停止タイマを開始します。
- 別のアクティブ状態のセカンダリサーバと通信しようとします。

サーバの停止タイマがタイムアウトとなった場合、サーバの状態は自動的にアクティブに変化します。タイマがタイムアウトする前にサーバをブロックの状態にした場合、そのサーバの状態は、手動で切り替えない限り自動的にはアクティブに戻ることはありません。すべてのセカンダリサーバが到達不能である場合、装置は認証あるいはアカウンティングに失敗します。

このコマンドは、プライマリ RADIUS 認証サーバに有効なテストプロファイルが指定されている場合に、RADIUS サーバのステータス検出機能に影響を与える可能性があります。

- サーバのステータスをブロックに設定すると、装置はサーバのステータスの検出を停止します。
- サーバのステータスをアクティブに設定すると、装置はサーバのステータスの検出を開始します。

例

RADIUS スキーム radius1 のすべてのセカンダリ認証サーバの状態を block に設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] state secondary authentication block

関連コマンド

- **display radius scheme**
- **state primary**

3.3.20 timer quiet (RADIUS scheme view)

Syntax

timer quiet *minutes*

undo timer quiet

デフォルト

5 分

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

minutes: サーバの停止タイマを指定します。設定範囲は 1〜255 です。

説明

timer quiet コマンドは RADIUS スキームの指定されたサーバの停止タイマを設定します。

undo timer quiet コマンドはデフォルトに戻します。

サーバの停止タイマが正しく設定されていることを確認してください。

タイマが短すぎる場合、装置がアクティブ状態の通信不能サーバと繰り返し通信しようとするため、頻繁に認証またはアカウンティングの失敗が発生します。

タイマが長すぎる場合、サーバの停止タイマが終了するまでサーバはブロック状態のままとなるため、故障から回復した到達可能なサーバを一時的にブロック状態にします。

例

RADIUS スキーム radius1 でサーバの停止タイマを 10 分に設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] timer quiet 10

関連コマンド

display radius scheme

3.3.21 timer realtime-accounting (RADIUS scheme view)

Syntax

timer realtime-accounting *interval* [**second**]

undo timer realtime-accounting

デフォルト

12 分

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

interval: リアルタイムのアカウンティング間隔を指定します。設定範囲は 0～71582 分です。

second: 計測単位を秒で指定します。このキーワードを指定しない場合、リアルタイムのアカウンティング間隔は分単位で測定されます。

説明

timer realtime-accounting コマンドはリアルタイムのアカウンティング間隔を設定します。

undo timer realtime-accounting コマンドはデフォルトに戻します。

装置のリアルタイムのアカウンティング間隔が 0 でないとき、装置は設定された間隔で RADIUS アカウンティングサーバにオンラインユーザのアカウンティング情報を送信します。

装置のリアルタイムのアカウンティング間隔が 0 であるとき、装置はサーバに設定されたリアルタイムのアカウンティング間隔で RADIUS アカウンティングサーバにオンラインユーザのアカウンティング情報を送信します。サーバでリアルタイムのアカウンティング間隔が設定されていない場合、装置はオンラインユーザのアカウンティング情報を送信しません。

ユーザが RADIUS アカウンティングを使用していて、RADIUS 認証および認可を使用していない場合、装置は、ユーザの RADIUS アカウンティングスキームで設定されたリアルタイムアカウンティング間隔に基づいてのみ、そのユーザのリアルタイムアカウンティングを実行します。RADIUS アカウンティングサーバによって割り当てられたリアルタイムアカウンティング間隔は有効になりません。

リアルタイムのアカウンティング間隔が短いと、アカウンティング情報の精度が上がりますが、多くのシステムリソースが必要となります。

表 3-6 リアルタイムのアカウンティング間隔の推奨値

ユーザ数	リアルタイムのアカウンティング間隔
1～99	3分
100～499	6分
500～999	12分
1000以上	15分以上

例

RADIUS スキーム radius1 のリアルタイムのアカウンティング間隔を 51 分に設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] timer realtime-accounting 51

関連コマンド

retry realtime-accounting

3.3.22 timer response-timeout (RADIUS scheme view)

Syntax

timer response-timeout *seconds*

undo timer response-timeout

デフォルト

3 秒

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

seconds: RADIUS サーバの応答タイムアウト時間を指定します。設定範囲は 1～10 秒です。

説明

timer response-timeout コマンドは RADIUS サーバの応答タイムアウトタイマを設定します。

undo timer response-timeout コマンドはデフォルトに戻します。

RADIUS 要求を送信した後、一定時間内に RADIUS サーバから応答がない場合、NAS はユーザが多くの RADIUS サービスを受ける機会を持てるように、RADIUS リクエストを再送します。NAS は、RADIUS サーバの応答タイムアウトタイマを使用して、この送信間隔を制御します。

クライアントが認証プロセスの間にタイムアウトした場合、ユーザはすぐにログオフします。ユーザのログオフを防ぐため、以下によって乗算した値は、アクセスモジュールによって定義したクライアントのタイムアウト時間よりも大きくすることができません。

- RADIUS パケットの最大試行回数
- RADIUS サーバ応答タイムアウト時間
- RADIUS スキームの RADIUS 認証サーバ数

装置が新しい RADIUS サーバに RADIUS 要求を送信するとき、RADIUS パケットを転送する総時間を確認してください。総時間が 300 秒を超過した場合、次の RADIUS サーバへの RADIUS 要求の送信を停止します。

パケットの再送試行回数と RADIUS サーバの応答タイムアウト時間を設定する際に、RADIUS サーバの数を考慮してください。

例

RADIUS スキーム radius1 の RADIUS サーバの応答タイムアウトタイマを 5 秒に設定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] timer response-timeout 5

関連コマンド

- **display radius scheme**
- **retry**

3.3.23 user-name-format (RADIUS scheme view)

Syntax

user-name-format { **keep-original** | **with-domain** | **without-domain** }

undo user-name-format

デフォルト

with-domain

View

RADIUS scheme view

定義済みユーザロール

network-admin

パラメータ

keep-original: RADIUS サーバに入力するユーザ名を送信します。

with-domain: RADIUS サーバに送信されるユーザ名に、ISP ドメイン名を含めます。

without-domain: RADIUS サーバに送信されるユーザ名から ISP ドメイン名を除外します。

説明

user-name-format コマンドは RADIUS サーバに送信されるユーザ名の形式を設定します。

undo user-name-format コマンドはデフォルトに戻します。

通常、ユーザ名の形式は *userid@isp-name* です。*isp-name* はユーザが所属する ISP ドメインを判断するために装置によって使用されます。しかし、旧型の RADIUS サーバの中には、ISP ドメイン名を含むユーザ名を認識できないものがあります。このような RADIUS サーバにドメイン名を含むユーザ名を送信する前に、装置はドメイン名を削除する必要があります。**user-name-format** コマンドを使用することで、RADIUS サーバに送信されるユーザ名にドメイン名を含めるかどうかを指定することができます。

RADIUS スキームが ISP ドメイン名を含まずにユーザ名を送信するよう定義している場合、この RADIUS スキームを複数の ISP ドメインに適用しないでください。これは、異なる 2 つの ISP ドメインに属する 2 つのユーザが、ユーザ ID が同じため、RADIUS サーバには 1 ユーザとみなされる、という混乱を避けるためです。

802.1X ユーザが EAP 認証を使用する場合、RADIUS スキームで設定された **user-name-format** コマンドは適用されません。RADIUS サーバに転送する際、装置はクライアントからユーザ名を変更できません。

例

RADIUS スキーム radius1 で、RADIUS サーバに送信されるユーザ名に、装置がドメイン名を削除するように指定します。

<AP> system-view

[AP] radius scheme radius1

[AP-radius-radius1] user-name-format without-domain

関連コマンド

display radius scheme

目次

このセクションのページは **12-x-x** です。

4 章 802.1X 4-1
4.1 802.1X 設定コマンド 4-1
4.1.1 display dot1x 4-1
4.1.2 display dot1x connection 4-7
4.1.3 dot1x 4-11
4.1.4 dot1x authentication-method 4-12
4.1.5 dot1x guest-vlan 4-13
4.1.6 dot1x handshake 4-14
4.1.7 dot1x handshake reply enable 4-15
4.1.8 dot1x mandatory-domain 4-16
4.1.9 dot1x max-user 4-17
4.1.10 dot1x multicast-trigger 4-18
4.1.11 dot1x port-control 4-19
4.1.12 dot1x port-method 4-20
4.1.13 dot1x quiet-period 4-21
4.1.14 dot1x re-authenticate 4-22
4.1.15 dot1x retry 4-23
4.1.16 dot1x timer 4-24
4.1.17 dot1x unicast-trigger 4-26
4.1.18 reset dot1x guest-vlan 4-27
4.1.19 reset dot1x statistics 4-28

4章 802.1X

4.1 802.1X設定コマンド

4.1.1 display dot1x

Syntax

display dot1x [**sessions** | **statistics**] [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

sessions: 802.1X のセッション接続情報を表示します。

statistics: 802.1X の統計情報を表示します。

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

説明

display dot1x コマンドは 802.1X についての情報を表示します。

sessions パラメータあるいは **statistics** パラメータのいずれのパラメータを指定しない場合、セッション情報、統計情報、設定情報を含む 802.1X のすべての情報を表示します。

例

802.1X のすべての情報を表示します。

<AP> display dot1x

```
Global 802.1X parameters:
   802.1X authentication  : Enabled
   CHAP authentication    : Enabled
   Max-tx period          : 30 s
   Handshake period       : 15 s
   Quiet timer            : Disabled
      Quiet period        : 60 s
   Supp timeout           : 30 s
   Server timeout         : 100 s
```

```
  Reauth period         : 3600 s
  Max auth requests     : 2
  SmartOn switch ID     : 30
  SmartOn supp timeout  : 30 s
  SmartOn retry counts  : 3
  EAD assistant function : Disabled
     URL              : http://www.dwsoft.com
     Free IP          : 6.6.6.0       255.255.255.0
     EAD timeout      : 30 min
  Domain delimiter     : @
Online 802.1X wired users   : 1
Online 802.1X wireless users : 1

GigabitEthernet1/0/1  is link-up
  802.1X authentication     : Enabled
  Handshake                 : Enabled
  Handshake reply           : Disabled
  Handshake security        : Disabled
  Unicast trigger           : Disabled
  Periodic reauth           : Disabled
  Port role                 : Authenticator
  Authorization mode        : Auto
  Port access control       : Port-based
  Multicast trigger         : Enabled
  Mandatory auth domain     : Not configured
  Guest VLAN                : 3
  Auth-Fail VLAN            : Not configured
  Critical VLAN             : Not configured
  Re-auth server-unreachable : Logoff
  Max online users          : 256
  SmartOn                   : Disabled

  EAPOL packets: Tx 3, Rx 3
  Sent EAP Request/Identity packets : 1
      EAP Request/Challenge packets: 1
      EAP Success packets: 1
      EAP Failure packets: 0
  Received EAPOL Start packets : 1
         EAPOL LogOff packets: 1
         EAP Response/Identity packets : 1
         EAP Response/Challenge packets: 1
         Error packets: 0
  Online 802.1X users: 1
```

```
        MAC address       Auth state
        0001-0000-0000     Authenticated

AP name: AP1  Radio ID: 1  SSID: wlan_dot1x_ssid
  BSSID                  : 1111-1111-1111
  802.1X authentication     : Enabled
  Handshake               : Enabled
  Handshake security       : Disabled
  Periodic reauth          : Disabled
  Mandatory auth domain     : Not configured
  Max online users         : 256

  EAPOL packets: Tx 3, Rx 3
  Sent EAP Request/Identity packets : 1
      EAP Request/Challenge packets: 1
      EAP Success packets: 1
      EAP Failure packets: 0
  Received EAPOL Start packets : 1
      EAPOL LogOff packets: 1
      EAP Response/Identity packets : 1
      EAP Response/Challenge packets: 1
      Error packets: 0
  Online 802.1X users: 1
       MAC address       Auth state
       0001-0000-0002     Authenticated
```

表 4-1 コマンド出力

フィールド	説明
Global 802.1X parameters	グローバル802.1Xの設定です。
802.1X authentication	802.1Xがグローバルで有効かどうかを示します。
CHAP authentication	RADIUSサーバと通信する際にEAPを終端しCHAPを実行しています。
EAP authentication	RADIUSサーバと通信する際にEAPパケットの中継とEAP認証のいずれかを実行しています。
PAP authentication	RADIUSサーバと通信する際にEAPを終端しPAPを実行しています。
Max-tx period	ユーザ名の要求タイムアウトタイマです。単位は秒です。
Handshake period	ハンドシェイクタイマです。単位は秒です。
Quiet timer	停止タイマの状態をenabledあるいはdisabledで示します。

フィールド	説明
Quiet period	停止タイマです。単位は秒です。
Supp timeout	クライアントタイムアウトタイマです。単位は秒です。
Server timeout	サーバタイムアウトタイマです。単位は秒です。
Reauth period	定期再認証タイマです。単位は秒です。
Max auth requests	認証要求をクライアントに送信する最大試行回数です。
SmartOn switch ID	SmartOn認証のSwitch IDです。
SmartOn supp timeout	SmartOnクライアントタイムアウトタイマです。単位は秒です。
SmartOn retry counts	EAP-Request/Notificationパケットをクライアントに再送する最大試行回数です。
EAD assistant function	EAP assistantが有効であるかを示します。
URL	認証されていないユーザがWebブラウザでネットワークに接続するためのリダイレクト用URLです。
Free IP	認証されていないユーザがアクセス可能なネットワークセグメントです。
EAD timeout	EADルールタイマです。単位は分です。
Domain delimiter	装置がサポートするドメインデリミタです。
Online 802.1X wired users	接続されたオンライン802.1Xユーザの数です。802.1X認証をパスしたユーザ、802.1X認証を実行しているユーザが含まれます。
Online 802.1X wireless users	802.1 X認証に合格したユーザおよび802.1 X認証を実行しているユーザを含む、ワイヤレスオンライン802.1 Xユーザの数です。
GigabitEthernet1/0/1 is link-up	ポートの状態です。たとえば、GigabitEthernet 1/0/1がupです。
802.1X authentication	802.1Xがポートで有効かを示します。
Handshake	オンラインユーザハンドシェイク機能がポートで有効かを示します。
Handshake reply	オンラインユーザハンドシェイク応答機能がポートで有効かを示します。
Handshake security	オンラインユーザハンドシェイクセキュリティ機能がポートで有効かを示します。
Unicast trigger	802.1Xユニキャストトリガがポートで有効かを示します。

フィールド	説明
Periodic reauth	定期オンラインユーザの再認証機能がポートで有効かを示します。
Port role	ポートの役割です。ポートは認証のみ機能します。
Authorization mode	ポートの許可状態です。 • **Force-Authorized** • **Auto** • **Force-Unauthorized**
Port access control	ポートのアクセス制御方式です。 • **MAC-based**—MACベースアクセス制御です。 • **Port-based**—ポートベースアクセス制御です。
Multicast trigger	802.1Xマルチキャストトリガ機能が有効かどうかを示します。
Mandatory auth domain	ポートの802.1X強制認証ドメインを示します。
Guest VLAN	ポートの802.1XゲストVLANを示します。 802.1XゲストVLANが設定されていない場合、**Not configured**と表示されます。
Auth-Fail VLAN	ポートの802.1X制限VLANを示します。 802.1X制限VLANが設定されていない場合、**Not configured**と表示されます。
Critical VLAN	ポートの802.1X critical VLANを示します。 802.1X critical VLANが設定されていない場合、**Not configured**と表示されます。
Re-auth server-unreachable	オンライン802.1Xがログオフしているか、802.1Xの再認証を行う際、サーバに到達不能状態であるかを示します。
Max online users	ポートの802.1Xユーザの同時接続最大数です。
SmartOn	ポートでSmartOn認証が有効かどうかを示します。
EAPOL packets	EAPOLパケットの送信数（Tx）および受信数（Rx）です。
Sent EAP Request/Identity packets	EAP-Request/Identityパケットの送信数です。
EAP Request/Challenge packets	EAP-Request/MD5 Challengeパケットの送信数です。
EAP Success packets	EAP-Successパケットの送信数です。
EAP Failure packets	EAP-Failureパケットの送信数です。
Received EAPOL Start packets	EAPOL-Startパケットの受信数です。

フィールド	説明
EAPOL LogOff packets	EAPOL-LogOffパケットの受信数です。
EAP Response/Identity packets	EAP-Response/Identityパケットの受信数です。
EAP Response/Challenge packets	EAP-Response/MD5 Challengeパケットの受信数です。
Error packets	エラーパケットの受信数です。
Online 802.1X users	ポートのオンライン802.1Xユーザ数です。 802.1X認証にパスしたユーザ、802.1X認証を実行しているユーザが含まれます。
MAC address	オンライン802.1XユーザのMACアドレスです。
Auth state	オンライン802.1Xユーザの認証状態です。

4.1.2 display dot1x connection

Syntax

display dot1x connection [**interface** *interface-type interface-number* | **user-mac** *mac-address* | **user-name** *name-string*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。ポートが指定されない場合、すべてのポートのオンライン 802.1X ユーザの情報を表示します。

user-mac *mac-address*: 802.1X ユーザの MAC アドレスを指定します。形式は H-H-H です。指定しない場合、すべての 802.1X ユーザの情報を表示します。

user-name *name-string*: 802.1X ユーザの名前を指定します。設定範囲は 1～253 文字です。大文字、小文字を区別します。指定しない場合、すべてのオンライン 802.1X ユーザの情報を表示します。

説明

display dot1x connection コマンドはオンライン 802.1X ユーザの情報を表示します。

例

すべてのオンライン 802.1X ユーザの情報を表示します。

<AP> display dot1x connection

```
Total connections: 1

User MAC address: 00ff-05a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
Authentication domain: abc
IPv4 address: 192.168.1.1
IPv6 address: 2000:0:0:0:1:2345:6789:abcd
Authentication method: CHAP
Initial VLAN: 1
Authorization untagged VLAN: 6
Authorization tagged VLAN list: 1 to 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33
29 31 33
```

```
                          35 37 40 to 100
Authorization ACL ID: 3001
Authorization user profile: N/A
Termination action: Default
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s

User MAC address             : 00ff-05a6-7cfe
AP name                     : ap1
Radio ID                    : 1
SSID                       : wlan_dot1x_ssid
BSSID                      : 0015-e9a6-7cf0
User name                   : ias
Authentication domain         : 1
IPv4 address                : 192.168.1.1
IPv6 address                : 2000:0:0:0:1:2345:6789:abcd
Authentication method         : CHAP
Initial VLAN                : 1
Authorization VLAN           : N/A
Authorization ACL number       : 3001
Authorization user profile     : N/A
Termination action           : Default
Session timeout period        : 2 sec
Online from                 : 2013/03/02 13:14:15
Online duration              : 0 h 2 m 15 s
```

表 4-2 コマンド出力

フィールド	説明
Total connections	オンライン802.1Xユーザの数です。
User MAC address	ユーザのMACアドレスです。
Access interface	ユーザが装置にアクセスするインタフェースです。
Authentication domain	802.1X認証で使用されるISPドメインです。
IPv4 address	ユーザのIPv4アドレスです。 装置がユーザのIPv4アドレスを取得できない場合、このフィールドは無効です。

フィールド	説明
Authentication method	EAPメッセージ操作方式です。 ● **CHAP**—RADIUSサーバと通信するEAPを終端しCHAPを実行しています。 ● **EAP**— RADIUSサーバと通信する際にEAPパケットの中継とEAP認証のいずれかを実行しています。 ● **PAP**—RADIUSサーバと通信する際にEAPを終端しPAPを実行しています。
Initial VLAN	802.1X認証を行う前にユーザが所属するVLANです。
Authorization untagged VLAN	ユーザに許可されたタグなしVLANです。
Authorization tagged VLAN list	ユーザに許可されたタグづけVLANです。
Authorization ACL number/name	ユーザに許可されたACLの番号または名前。 許可されたACLがない場合、このフィールドには**N/A**と表示されます。 ACL許可が失敗した場合、このフィールドにはACL番号または名前の後に **(Not effective)** と表示されます。
Authorization user profile	ユーザに許可されたユーザプロファイルです。
Authorization CAR	サーバによって割り当てられた認可CAR属性です。 ● **Average input rate**—信トラフィックの平均レート (bps単位)です。 ● **Average output rate**—信トラフィックの平均レート (bps単位)です。 認可CAR属性が割り当てられていない場合、このフィールドには**N/A**と表示されます。
Authorization URL	ユーザに許可されたリダイレクトURLです。
Termination action	セッションタイムアウトタイマが終了したときにサーバに割り当てられたアクションです。 ● **Default**—認証されたオンライン802.1Xユーザをログオフします。定期オンラインユーザの再認証が有効で、セッションタイムアウトタイマより定期再認証タイマが短い場合は、適用されません。 ● **Radius-request**—セッションタイムアウトタイマが終了したとき、定期オンラインユーザの再認証の設定に関わらず、オンラインユーザを再認証します。 装置がローカル認証を実行するとき、このフィールドは**N/A**と表示されます。

フィールド	説明
Session timeout period	サーバによって割り当てられたセッションタイムアウトタイマです。 装置がローカル認証を実行する場合、このフィールドには**N/A**と表示されます。
Online from	802.1Xユーザがオンラインになったとき時間です。
Online duration	802.1Xユーザがオンラインになってからの経過時間です。
Level flow statistic	各アカウンティングレベルのトラフィックフローに関する統計情報です。 ● **Level-n**—トラフィックアカウンティングレベル。使用可能なレベルは、レベル0~レベル8です。アカウンティングレベルは、WLANアカウンティングポリシーで定義されます。 ● **Sent packets/bytes**—送信パケット数および送信バイト数です。 ● **Received packets/bytes**—受信パケット数および受信バイト数です。

4.1.3 dot1x

Syntax

dot1x

undo dot1x

デフォルト

802.1X はグローバルおよびポートで無効です。

View

System view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x コマンドは 802.1X をグローバルあるいはポートで有効にします。

undo dot1x コマンドは 802.1X をグローバルあるいはポートで無効にします。

802.1X はグローバルとポートの両方で有効にする必要があります。そうでない場合、動作しません。

例

802.1X をグローバルで有効にします。

<AP> system-view

[AP] dot1x

GigabitEthernet 1/0/1 で 802.1X を有効にします。

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x

[AP-GigabitEthernet1/0/1] quit

関連コマンド

display dot1x

4.1.4 dot1x authentication-method

Syntax

dot1x authentication-method { **chap** | **eap** | **pap** }

undo dot1x authentication-method

デフォルト

chap

View

System view

定義済みユーザロール

network-admin

パラメータ

chap: RADIUS サーバと通信するために EAP（Extensible Authentication Protocol）を終端し、CHAP（Challenge Handshake Authentication Protocol）認証を使用します。

eap: RADIUS サーバと通信するために、EAP パケットを中継し、EAP 認証をサポートします。

pap: RADIUS サーバと通信するために、EAP を終端し、PAP（Password Authentication Protocol）認証をサポートします。

説明

dot1x authentication-method コマンドは EAP メッセージ操作方法を指定することで 802.1X ユーザの認証方法を設定します。

undo dot1x authentication-method コマンドはデフォルトに戻します。

装置は EAP パケットを終端する、あるいは中継します。

- **EAP 終端モード**—アクセス装置は標準の RADIUS パケットの認証データを再カプセル化し、クライアントから RADIUS サーバに送信します。装置は RADIUS サーバの CHAP あるいは PAP 認証のどちらかを実行します。このモードでは RADIUS サーバは MD5-チャレンジ EAP 認証のみをサポートします。
  - □ PAP はプレーンテキストでユーザ名とパスワードを転送します。この認証方法は高いセキュリティを必要としないシナリオに適用します。
  - □ CHAP はネットワークを越えてプレーンテキストのユーザ名と暗号化されたパスワードを転送します。CHAP は PAP よりもセキュリティが高いです。
- EAP 中継モード－アクセス装置はクライアントと RADIUS サーバ間の EAP メッセージを中継します。EAP 中継モードは MD5-チャレンジ、EAP-TLS、PEAP のような複数の EAP 認証方式をサポートします。このモードを使用するため、RADIUS サーバは以下の要件に適用する必要があります。

- EAP メッセージとメッセージ-認証属性をサポートします。
- クライアントとして同じ EAP 認証方式を使用します。

このモードが使用されると、RADIUS scheme view で **user-name-format** コマンドは適用されません。**user-name-format** コマンドについての詳細は、コマンドマニュアルのセクション 12 *ユーザアクセスと認証 “AAA”* を参照してください。

RADIUS 認証が使用されると、RADIUS サーバとして同じ認証方式（PAP、CHAP、EAP）を使用するようにアクセス装置を設定する必要があります。

例

EAP パケットを終端するアクセス装置を有効にし、RADIUS サーバで PAP 認証を実行します。

<AP> system-view

[AP] dot1x authentication-method pap

関連コマンド

display dot1x

4.1.5 dot1x guest-vlan

Syntax

dot1x guest-vlan *guest-vlan-id*

undo dot1x guest-vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

guest-vlan-id: 802.1X ゲスト VLAN の ID を指定します。設定範囲は 1～4094 です。VLAN が作成されている必要があります。

説明

dot1x guest-vlan コマンドはポートで 802.1X ゲスト VLAN を設定します。

undo dot1x guest-vlan コマンドは デフォルトに戻します。

802.1X ゲスト VLAN は 802.1X 認証を実行していないユーザに適用されます。ユーザは 802.1X ゲスト VLAN で、アンチウィルスソフトウェアをダウンロードするため、ソフトウェアサーバなどの制限されたネットワークリソースを使用します。

802.1X ゲスト VLAN として設定された VLAN を削除する場合、最初に **undo dot1x guest-vlan** コマンドを使用します。

802.1X ゲスト VLAN の詳細についてはオペレーションマニュアルのセクション *12 ユーザアクセスと認証関連 "802.1X の設定"* を参照してください。

例

GigabitEthernet 1/0/1 で 802.1X ゲスト VLAN100 を設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x guest-vlan 100

関連コマンド

display dot1x

4.1.6 dot1x handshake

Syntax

dot1x handshake

undo dot1x handshake

デフォルト

有効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x handshake コマンドはオンラインユーザハンドシェイク機能を有効にします。

undo dot1x handshake コマンドは機能を無効にします。

オンラインユーザハンドシェイク機能は、オンライン 802.1X ユーザの接続状態を確認するため、装置が定期的にハンドシェイクメッセージをクライアントに送信することを有効にします。もし装置がハンドシェイクタイマの時間に、ハンドシェイクの最大試行回数を実行してもオンラインユーザからの応答を受信しない場合、ユーザをオフライン状

態に設定します。ハンドシェイクタイマを設定する場合、**dot1x timer handshake-period** コマンドを使用します。ハンドシェイクの最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。

例

GigabitEthernet 1/0/1 でオンラインユーザハンドシェイク機能を有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x handshake

関連コマンド

- **display dot1x**
- **dot1x timer handshake-period**
- **dot1x retry**

4.1.7 dot1x handshake reply enable

Syntax

dot1x handshake reply enable

undo dot1x handshake reply enable

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x handshake reply enable コマンドはハンドシェイクリプライ機能を有効にします。

undo dot1x handshake reply enable コマンドはハンドシェイクリプライ機能を無効にします。

dot1x handshake reply enable コマンドは、オンラインハンドシェイク処理中に、802.1X クライアントの EAP-Response/Identity パケットに応答するため、EAP-Success パケットを使用することを有効にします。

802.1X クライアントが装置から EAP-Success パケットを受信しないでオフラインになった場合のみ使用します。

例

GigabitEthernet 1/0/1 でハンドシェイクリプライ機能を設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x handshake reply enable

関連コマンド

dot1x handshake

4.1.8 dot1x mandatory-domain

Syntax

dot1x mandatory-domain *domain-name*

undo dot1x mandatory-domain

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

domain-name: ドメイン名を指定します。設定範囲は 1～255 です。大文字、小文字を区別しません。

説明

dot1x mandatory-domain コマンドはポートで強制 802.1X 認証ドメインを指定します。

undo dot1x mandatory-domain コマンドは強制 802.1X 認証ドメインを削除します。

システムがポートにアクセスを行う 802.1X ユーザの認証を行うとき、以下の順番で認証ドメインを選択します。

1) 強制ドメイン
2) ユーザ名で指定された ISP ドメイン
3) デフォルト ISP ドメイン

例

GigabitEthernet 1/0/1 で 802.1X ユーザに強制 802.1X 認証ドメインを設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x mandatory-domain my-domain

関連コマンド

display dot1x

4.1.9 dot1x max-user

Syntax

dot1x max-user *max-number*

undo dot1x max-user

デフォルト

4294967295

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

max-number: ポートで 802.1X ユーザが同時に接続する最大数を指定します。設定範囲は 1～4294967295 です。

説明

dot1x max-user コマンドはポートで 802.1X ユーザが同時に接続する最大数を指定します。

undo dot1x max-user コマンドはデフォルトに戻します。

システムリソースが乱用されることを防止するため、ポートで 802.1X ユーザが同時に接続する最大数を設定します。最大数に到達したとき、ポートで後続の 802.1X ユーザは拒否されます。

例

GigabitEthernet 1/0/1 で 802.1X ユーザが同時に接続する最大数を 32 に指定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x max-user 32

関連コマンド

display dot1x

4.1.10 dot1x multicast-trigger

Syntax

dot1x multicast-trigger

undo dot1x multicast-trigger

デフォルト

有効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x multicast-trigger コマンドは 802.1X マルチキャストトリガ機能を有効にします。

undo dot1x multicast-trigger コマンドは機能を無効にします。

802.1X マルチキャストトリガ機能は装置がイニシエータとして動作することを有効にします。装置は 802.1X クライアントを検出し、認証を開始するため、定期的に EAP-Request/Identity パケットをマルチキャストします。マルチキャスト EAP-Request/Identity パケットを送信する間隔を設定するため、**dot1x timer tx-period** コマンドを使用します。

無線 LAN ではマルチキャストトリガ機能を無効にします。無線クライアントとアクセス装置の無線モジュールはそれぞれ 802.1X 認証を開始することができます。

例

GigabitEthernet 1/0/1 で 802.1X マルチキャストトリガ機能を有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x multicast-trigger

関連コマンド

- **display dot1x**
- **dot1x timer tx-period**
- **dot1x unicast-trigger**

4.1.11 dot1x port-control

Syntax

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

デフォルト

auto

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

authorized-force: ポートを許可された状態に設定します。認証を行わずネットワークにアクセスできるようにポートのユーザを有効にします。

auto: 指定されたポートあるいはすべてのポートを最初は EAPOL フレームだけは通す許可されていない状態に設定し、認証に成功した後は、ネットワークへのアクセスを許可する許可状態に変更します。これが最も一般的な使用方法です。

unauthorized-force: ポートを許可されていない状態に設定します。ポートのユーザからのアクセス要求を拒否します。

説明

dot1x port-control コマンドはポートの許可状態を設定します。

undo dot1x port-control コマンドはデフォルトに戻します。

このコマンドを使用することで、クライアントのネットワークへのアクセスを許可されるかどうかを決定するため、ポートに許可状態を設定することができます。

例

GigabitEthernet 1/0/1 の許可状態を unauthorized-force に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x port-control unauthorized-force

関連コマンド

display dot1x

4.1.12 dot1x port-method

Syntax

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

デフォルト

macbased

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

macbased: MAC ベースアクセス制御方式を使用します。この方式はポートのそれぞれのユーザを個別に認証します。認証されたユーザがログオフしたとき、この方式を使用しても、他のオンラインユーザには影響しません。

portbased: ポートでポートベースアクセス制御方式を使用します。この方式はポートで最初のユーザが認証に成功すると他のすべてのユーザが認証なしでネットワークへアクセスすることができます。最初のユーザがログオフになったとき、同時に他のすべてのユーザもログオフになります。

説明

dot1x port-method コマンドはポートのアクセス制御方式を指定します。

undo dot1x port-method コマンドはデフォルトに戻します。

⚠ **注意:**

ポートにオンライン 802.1 X ユーザが存在する場合、そのアクセス制御方式を変更すると、オンラインユーザがオフラインになります。

ポートで 802.1X 認証、ポータル認証を使用する場合、MAC ベースアクセス制御方式にする必要があります。

例

GigabitEthernet 1/0/1 をポートベースアクセス制御方式に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x port-method portbased

関連コマンド

display dot1x

4.1.13 dot1x quiet-period

Syntax

dot1x quiet-period

undo dot1x quiet-period

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

dot1x quiet-period コマンドは停止タイマを有効にします。

undo dot1x quiet-period コマンドは停止タイマを無効にします。

クライアントが 802.1X 認証に失敗したとき、装置は、クライアントから認証要求を処理する前に、一定期間を待つ必要があります。停止タイマの時間を設定する場合、**dot1x timer quiet-period** コマンドを使用します。

例

停止タイマを有効にし、停止時間を 100 秒に設定します。

<AP> system-view

[AP] dot1x quiet-period

[AP] dot1x timer quiet-period 100

関連コマンド

- **display dot1x**
- **dot1x timer**

4.1.14 dot1x re-authenticate

Syntax

dot1x re-authenticate

undo dot1x re-authenticate

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x re-authenticate コマンドは定期的なオンラインユーザの再認証機能を有効にします。

undo dot1x re-authenticate コマンドは機能を無効にします。

定期再認証機能を有効にすると、アクセス装置は、ポートのオンライン 802.1X ユーザを定期的に認証します。この機能はオンラインユーザの接続状態を確認し、ACL や VLAN などの、サーバに割り当てられた許可属性をアップデートします。

再認証を行う期間を設定する場合、**dot1x timer reauth-period** コマンドを使用します。

例

GigabitEthernet 1/0/1 で 802.1X オンラインユーザの再認証機能を有効にし、再認証を行う期間を 1800 秒に設定します。

<AP> system-view

[AP] dot1x timer reauth-period 1800

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x re-authenticate

関連コマンド

- **display dot1x**
- **dot1x timer**

4.1.15 dot1x retry

Syntax

dot1x retry *retries*

undo dot1x retry

デフォルト

2

View

System view

定義済みユーザロール

network-admin

パラメータ

retries: クライアントに認証要求を送信する最大試行回数を指定します。設定範囲は 1～10 です。

説明

dot1x retry コマンドはクライアントに認証要求を送信する最大試行回数を設定します。

undo dot1x retry コマンドはデフォルトに戻します。

以下のいずれかの状況により、アクセス装置はクライアントに認証要求を再送します。

- 装置はユーザ名の要求タイマ内にクライアントから応答を受信しません。EAP-Request/Identity パケットのタイマは **dot1x timer tx-period** *tx-period-value* コマンドで設定することができます。
- 装置はクライアントタイムアウトタイマ内にクライアントから応答を受信しません。EAP-Request/MD5-Challenge パケットのタイマは **dot1x timer supp-timeout** *supp-timeout-value* コマンドで設定することができます。

認証要求を送信する試行回数が最大に到達しても応答を受信しない場合、アクセス装置は要求の再送を停止します。

例

クライアントに認証要求を送信する最大試行回数を 9 に設定します。

<AP> system-view

[AP] dot1x retry 9

関連コマンド

- **display dot1x**
- **dot1x timer**

4.1.16 dot1x timer

Syntax

dot1x timer { **ead-timeout** *ead-timeout-value* | **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **ead-timeout** | **handshake-period** | **quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period** }

デフォルト

- EAD ルールタイマ：30 分
- ハンドシェイクタイマ：15 秒
- 停止タイマ：60 秒
- 定期再認証タイマ：3600 秒
- サーバタイムアウトタイマ：100 秒
- クライアントタイムアウトタイマ：30 秒
- ユーザ名要求タイムアウトタイマ：30 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

ead-timeout *ead-timeout-value*: EAD のルールタイマを分単位で設定します。設定範囲は 1～1440 です。

handshake-period *handshake-period-value*: ハンドシェイクタイマを設定します。設定範囲は 5～1024 秒です。

quiet-period *quiet-period-value*: 停止タイマを設定します。設定範囲は 10～120 秒です。

reauth-period *reauth-period-value*: 定期再認証タイマを設定します。設定範囲は 60～7200 秒です。

server-timeout *server-timeout-value*: サーバタイムアウトタイマを設定します。設定範囲は 100～300 秒です。

supp-timeout *supp-timeout-value*: クライアントタイムアウトタイマを設定します。設定範囲は 1～120 秒です。

tx-period *tx-period-value*: ユーザ名要求タイムアウトタイマを設定します。設定範囲は 1～120 秒です。

説明

dot1x timer コマンドは 802.1X タイマを設定します。

undo dot1x timer コマンドはデフォルトに戻します。

ほとんどの状況ではデフォルトの設定で十分です。ネットワークの状況に依存してタイマを設定することができます。

- 低速ネットワークでは、クライアントタイムアウトタイマを増加します。
- 脆弱なネットワークでは、停止タイマの値を大きい値に設定します。
- 認証の応答が早急な高性能ネットワークでは、停止タイマを小さい値に設定します。
- 異なる性能の認証サーバがあるネットワークではサーバタイムアウトタイマを適切に設定します。

ネットワーク装置は以下の 802.1X タイマを使用します。

- **EAD ルールタイマ (ead-timeout)** – 各 EAD ルールのライフタイムを設定します。タイマの期限が切れるか、ユーザが認証に合格すると、ルールは削除されます。ユーザが EAD クライアントのダウンロードに失敗した場合、またはタイマ間隔内に認証に合格しなかった場合、ユーザはネットワークに再接続して空き IP にアクセスする必要があります。
- **ハンドシェイクタイマ（handshake-period）**－装置が認証ユーザのオンライン状況の確認のためハンドシェイク要求を定期的に送信する間隔を設定します。ハンドシェイク要求に応答がない場合には、認証ユーザがログオフしたと判断します。
- **停止タイマ（quiet-period）**—クライアントが認証に失敗したとき開始します。アクセス装置はクライアントから認証処理を開始する前に、タイマの時間を待つ必要があります。
- **定期再認証タイマ（reauth-period）**—ポート上の定期再認証を有効にすると、装置は、タイマで設定された間隔でポート上のオンラインユーザを再認証します。この設定は **dot1x re-authenticate** コマンドで設定します。
- **サーバタイムアウトタイマ（server-timeout）**—アクセス装置が認証サーバに RADIUS Access-Request パケットを送信するときに開始します。このタイマが時間切れになるまでに応答がなかった場合、アクセス装置は、サーバに要求を再送します。
- **クライアントタイムアウトタイマ（supp-timeout）**—アクセス装置がクライアントに EAP-Request/MD5 Challenge パケットを送信するときに開始します。このタイマが時間切れになるまで応答がなかった場合、アクセス装置は、クライアントに要求を再送します。
- **ユーザ名要求タイムアウトタイマ（tx-period）**—装置が EAP-Request/Identity パケットをクライアントに認証要求の応答として送信するときに開始します。タイマが終了する前に装置が応答を受信しない場合、要求を再送します。認証をアクティブに要求できないクライアントを検出するため、EAP-Request/Identity パケットをネットワーク装置に、設定されたタイマの間隔でマルチキャストします。

定期再認証タイマは古い再認証タイマが終了した後、新しく設定された再認証の間隔が適用されます。他のタイマは設定を変更するとすぐに適用されます。

例

サーバタイムアウトタイマを 150 秒に設定します。

<AP> system-view

[AP] dot1x timer server-timeout 150

関連コマンド

display dot1x

4.1.17 dot1x unicast-trigger

Syntax

dot1x unicast-trigger

undo dot1x unicast-trigger

デフォルト

無効

View

Ethernet interface view

定義済みユーザロール

network-admin

説明

dot1x unicast-trigger コマンドは 802.1X ユニキャストトリガ機能を有効にします。

undo dot1x unicast-trigger コマンドは 802.1X ユニキャストトリガ機能を無効にします。

802.1X ユニキャストトリガ機能は、未知の送信元 MAC アドレスからデータフレームを受信したときに 802.1X 認証を開始する機能です。装置は、ユニキャスト EAP-Request/Identity パケットを未知の送信元の MAC アドレスに送信しますが、一定時間内（**dot1x timer tx-period** コマンドで指定されます）に反応がない場合、パケットを再送します。このプロセスはで設定された最大試行回数（**dot1x retry** コマンドで指定されます)、実施します。

例

GigabitEthernet 1/0/1 のユニキャストトリガ機能を有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] dot1x unicast-trigger

関連コマンド

- **display dot1x**
- **dot1x multicast-trigger**
- **dot1x retry**
- **dot1x timer**

4.1.18 reset dot1x guest-vlan

Syntax

reset dot1x guest-vlan interface *interface-type interface-number* [**mac-address** *mac-address*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。

mac-address *mac-address*: ゲスト VLAN の 802.1X ユーザの MAC アドレスを指定します。指定しない場合、ポートのすべての 802.1X ユーザを削除します。

説明

reset dot1x guest-vlan コマンドはポートの 802.1X ゲスト VLAN からユーザを削除します。

例

GigabitEthernet 1/0/1 の 802.1X ゲスト VLAN から MAC アドレスが 1-1-1 のユーザを削除します。

<AP> reset dot1x guest-vlan interface gigabitethernet 1/0/1 mac-address 1-1-1

関連コマンド

dot1x guest-vlan

4.1.19 reset dot1x statistics

Syntax

reset dot1x statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定されない場合、すべてのポートの 802.1X の統計情報を削除します。

説明

reset dot1x statistics コマンドはポートの 802.1X の統計情報を削除します。

例

GigabitEthernet 1/0/1 の 802.1X の統計情報を削除します。

<AP> reset dot1x statistics interface gigabitethernet 1/0/1

関連コマンド

display dot1x

目次

このセクションのページは **12-x-x** です。

5 章 MAC アドレス認証 5-1
5.1 MAC アドレス認証設定コマンド 5-1
5.1.1 display mac-authentication 5-1
5.1.2 display mac-authentication connection 5-5
5.1.3 mac-authentication 5-8
5.1.4 mac-authentication authentication-method 5-9
5.1.5 mac-authentication domain 5-10
5.1.6 mac-authentication max-user 5-11
5.1.7 mac-authentication timer 5-12
5.1.8 mac-authentication user-name-format 5-13
5.1.9 reset mac-authentication statistics 5-15

5章 MAC アドレス認証

5.1 MACアドレス認証設定コマンド

5.1.1 display mac-authentication

Syntax

display mac-authentication [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのグローバルと指定したポートの MAC アドレス認証の情報を表示します。

説明

display mac-authentication コマンドは MAC アドレス認証の設定と統計情報を表示します。グローバルの設定、指定したポートに関する設定、MAC アドレス認証の統計情報、オンラインユーザの統計情報を表示します。

例

すべての MAC アドレス認証の設定と統計情報を表示します。

<AP> display mac-authentication

```
Global MAC authentication parameters:
  MAC authentication     : Enabled
  User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
         Username       : mac
         Password       : Not configured
  Offline detect period  : 300 s
  Quiet period          : 60 s
  Server timeout        : 100 s
  Authentication domain  : Not configured, use default domain
 Online MAC-auth wired users    : 1
 Online MAC-auth wireless users : 2
```

```
Silent MAC users:
        MAC address      VLAN ID  From port             Port index
        0001-0000-0001    100     GigabitEthernet1/0/2   21
        0001-0000-0003    12      GigabitEthernet1/0/4   301

GigabitEthernet1/0/1  is link-up
  MAC authentication        : Enabled
  Carry User-IP            : Disabled
  Authentication domain     : Not configured
  Auth-delay timer          : Enabled
     Auth-delay period      : 60 s
  Re-auth server-unreachable : Logoff
  Host mode                : Multiple VLAN
  Max online users          : 256
  Authentication attempts    : successful 2, failed 3
  Current online users      : 1
        MAC address      Auth state
        0001-0000-0000    Authenticated
        0001-0000-0001    Unauthenticated

AP name: AP1  Radio ID: 1  SSID: wlan_maca_ssid
  BSSID                    : 1111-1111-1111
  MAC authentication        : Enabled
  Authentication domain     : Not configured
  Max online users          : 256
  Authentication attempts    : successful 1, failed 0
  Current online users      : 2
        MAC address      Auth state
        0001-0000-0002    Authenticated
        0001-0000-0003    Unauthenticated
```

表 5-1 コマンド出力

フィールド	説明
MAC authentication	MACアドレス認証がグローバルで有効かどうかを示します。
Authentication method	MAC認証の認証方式:CHAPまたはPAPです。
User name format	ユーザアカウントタイプです。MACベースあるいは共有があります。 • MACベースアカウントが使用される場合、ユーザ名のフォーマットで表示されます。たとえば、ハイフンなし、16進数表示、小文字でMACアドレスが**MAC address in**

フィールド	説明
	lowercase(xx-xx-xx-xx-xx-xx)と表示されます。 ● 共有アカウントが使用される場合、**Fixed account**と表示されます。
User name	MACアドレス認証のユーザ名です。 ● MACベースアカウントが使用される場合、**mac**と表示されます。装置はMACアドレス認証のユーザ名とパスワードとして各ユーザのMACアドレスを使用します。 ● 共有アカウントが使用される場合、MACアドレス認証ユーザの共有アカウントのユーザ名が表示されます。デフォルトのユーザ名は**mac**です。
Password	MACアドレス認証のパスワードです。 ● MACベースアカウントが使用されている場合、あるいは共有アカウントでパスワードが設定されていない場合、**Not configured**と表示されます。 ● 共有アカウントでパスワードが設定されている場合、とアスタリスク（******）の文字列が表示されます。
Offline detect period	オフライン検出タイマです。
Quiet period	Quietタイマです。
Server timeout	サーバタイムアウトタイマです。
Authentication domain	system viewで指定されたMACアドレス認証のドメインです。system viewでMACアドレス認証のドメインが指定されていない場合、**Not configured, use default domain**と表示されます。
Online MAC-auth wired users	MACアドレス認証の接続されたオンラインユーザ数です。MACアドレス認証にパスしたユーザとMACアドレス認証を実行しているユーザが含まれます。
Online MAC-auth wireless users	MAC認証に合格したユーザおよびMAC認証を実行しているユーザを含む、ワイヤレスオンラインMAC認証ユーザの数です。
Silent MAC users	サイレントMACアドレスについての情報です。
MAC address	サイレントMACアドレスです。
VLAN ID	サイレントMACアドレスが所属するVLANのIDです。
From port	サイレントMACアドレスとしてMACアドレスを記載するポート名です。
Port index	サイレントMACアドレスとしてMACアドレスを記載するポートのインデックスです。

フィールド	説明
GigabitEthernet1/0/1 is link-up	GigabitEthernet 1/0/1のリンクの状態です。この例ではリンクがupしています。
MAC authentication	MACアドレス認証がポートで有効かどうかを示します。
Carry User-IP	MACアドレス認証要求にユーザのIPアドレスが含まれるかどうかを示します。このフィールドは現在のソフトウェアバージョンでサポートしていません。
Authentication domain	ポートのために指定されたMACアドレス認証のドメインです。
Auth-delay timer	MACアドレス認証の開始を遅らせる機能が有効かどうかを示します。
Auth-delay period	MACアドレス認証の開始を遅らせる遅延時間のタイマです。
Re-auth server-unreachable	サーバが到達不能であるときのMACアドレス認証の再認証を行う際のアクションです。 ● **Logoff**—オンラインユーザをログオフします。 ● **Online**—MACアドレス認証ユーザのログインを保持します。
Guest VLAN	ポートに設定されたMAC認証ゲストVLANです。 MAC認証ゲストVLANが設定されていない場合、このフィールドには**Not configured**と表示されます。
Guest VLAN auth-period	ポート上のMAC認証ゲストVLANのユーザの認証間隔です。
Critical VLAN	ポートに設定されたMAC認証クリティカルVLAN。 MAC認証クリティカルVLANが設定されていない場合、このフィールドには**Not configured**と表示されます。
Host mode	● マルチVLANモードが無効の場合、**Single VLAN**と表示されます。 ● マルチVLANモードが無効の場合、**Multiple VLAN**と表示されます。
Max online users	ポートで許可されたオンラインユーザの同時接続最大数です。
Authentication attempts: successful 1, failed 0	MACアドレス認証の統計情報です。MACアドレス認証に成功した試行回数、認証に失敗した試行回数です。
MAC address	オンラインユーザのMACアドレスです。
Auth state	ユーザの状態です。 ● **Authenticated**—ユーザがMACアドレス認証に成功しています。 ● **Unauthenticated**—ユーザがMACアドレス認証に失敗しています。

5.1.2 display mac-authentication connection

Syntax

display mac-authentication connection [**interface** *interface-type interface-number* | **user-mac** *mac-addr* | **user-name** *user-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのポートのオンライン MAC アドレス認証ユーザの情報を表示します。

user-mac *mac-address*: オンライン MAC アドレス認証ユーザの MAC アドレスです。*mac-address* はユーザの MAC アドレスを示します。形式は H-H-H です。指定しない場合、すべてのオンライン MAC アドレス認証ユーザの情報を表示します。

user-name *user-name*: オンライン MAC アドレス認証ユーザのユーザ名です。設定範囲は 1～253 文字です。大文字、小文字を区別します。ドメイン名を含むことができます。指定しない場合、すべてのオンライン MAC アドレス認証ユーザの情報を表示します。

説明

display mac-authentication connection コマンドはオンライン MAC アドレス認証ユーザの情報を表示します。

例

すべてのオンライン MAC アドレス認証ユーザの情報を表示します。

<AP> display mac-authentication connection

```
Total connections: 1

User MAC address: 00ff-10a6-7cfe
Access interface: GigabitEthernet1/0/1
Username: ias
Authentication domain: abc
Initial VLAN: 1
Authorization untagged VLAN: 100
Authorization tagged VLAN: N/A
Authorization ACL ID: 3001
Authorization user profile: N/A
```

```
Authorization URL: N/A
Termination action: Radius-request
Session timeout period: 2 s
Online from: 2013/03/02  13:14:15
Online duration: 0h 2m 15s

User MAC address            : 00ff-10a6-7cfe
AP name                    : ap1
Radio ID                   : 1
SSID                      : wlan_dot1x_ssid
BSSID                     : 00ff-99a6-7cf0
User name                  : ias
Authentication domain        : 1
Initial VLAN               : 1
Authorization VLAN          : 100
Authorization ACL number     : 3001
Authorization user profile    : N/A
Authorization URL           : N/A
Termination action          : Radius-request
Session timeout period       : 2 sec
Online from                : 2014/06/02 13:14:15
Online duration             : 0h 2m 15s
```

表 5-2 コマンド出力

フィールド	説明
Total connections	オンラインMACアドレス認証ユーザの総数です。
User MAC address	ユーザのMACアドレスです。
Access interface	ユーザが装置にアクセスするインタフェースです。
Authentication domain	ユーザが所属するMACアドレス認証のドメインです。
Authentication method	適用された認証の方式です。
IPv4 address	ユーザのIPv 4アドレスです。 使用可能なユーザIPv 4アドレスがない場合、このフィールドは表示されません。
Initial VLAN	MACアドレス認証を行う前にユーザを保持するVLANです。
Authorization untagged VLAN	有線ユーザに許可されたタグなしVLANです。
Authorization tagged VLAN	有線ユーザに許可されたタグつきVLANです。

フィールド	説明
Authorization VLAN	ユーザに許可されたVLANです。
Authorization ACL number/name	ユーザに許可されたACLの番号または名前です。 許可されたACLがない場合、このフィールドには**N/A**と表示されます。 ACL許可が失敗した場合、このフィールドはACL番号または名前の後に **(NOT effective)** と表示されます
Authorization user profile	ユーザに許可されたユーザプロファイルです。
Authorization CAR	サーバによって割り当てられた認可CAR属性。 ● **Average input rate**—着信トラフィックの平均レート (bps 単位)。 ● **Average output rate**—発信トラフィックの平均レート (bps 単位) 認可CAR属性が割り当てられていない場合、このフィールドには**N/A**と表示されます。
Termination action	セッションタイムアウトタイマが終了したとき、サーバに割り当てられたアクションの属性です。 ● **Default**—セッションタイムアウトタイマが終了したときオンライン認証ユーザをログオフします。 ● **Radius-request**—セッションタイムアウトタイマが終了したとき、オンラインユーザを再認証します。 ローカル認証が実行されている場合、**N/A**と表示されます。
Session timeout period	サーバによって割り当てられたセッションタイムアウトタイマです。
Online from	MACアドレス認証ユーザがオンラインになった時間です。
Online duration	MACアドレス認証ユーザがオンラインになってからの経過時間です。

5.1.3 mac-authentication

Syntax

mac-authentication

undo mac-authentication

デフォルト

無効

View

System view

Ethernet interface view

定義済みユーザロール

network-admin

説明

mac-authentication コマンドはグローバルあるいはポートで MAC アドレス認証を有効にします。

undo mac-authentication コマンドはグローバルあるいはポートで MAC アドレス認証を無効にします。

ポートで MAC アドレス認証を使用する場合、グローバルとポートの両方で MAC アドレス認証を有効にする必要があります。

例

グローバルで MAC アドレス認証を有効にします。

<AP> system-view

[AP] mac-authentication

GigabitEthernet 1/0/1 で MAC アドレス認証を有効にします。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] mac-authentication

関連コマンド

display mac-authentication

5.1.4 mac-authentication authentication-method

Syntax

mac-authentication authentication-method { chap | pap }

undo mac-authentication authentication-method

デフォルト

RADIUS サーバとの通信に PAP を使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

chap: RADIUS サーバとの通信に Challenge Handshake Authentication Protocol (CHAP) を使用します。

pap: RADIUS サーバとの通信に Password Authentication Protocol (PAP) を使用します。

説明

mac-authentication authentication-method コマンドは MAC アドレス認証の認証方式を設定します。

undo mac-authentication authentication-method コマンドはデフォルトに戻します。

RADIUS ベースの MAC 認証では、次の認証方式がサポートされています。

- PAP:ユーザ名とパスワードをプレーンテキストで転送します。認証方法は、高度なセキュリティを必要としないシナリオに適用されます。
- CHAP:ユーザ名をプレーンテキストで、パスワードを暗号化してネットワーク経由で転送します。CHAP は PAP よりも安全です。

例

MAC 認証に CHAP を使用するようにデバイスを設定します。

<AP> system-view

[AP] mac-authentication authentication-method chap

関連コマンド

display mac-authentication

5.1.5 mac-authentication domain

Syntax

mac-authentication domain *domain-name*

undo mac-authentication domain

デフォルト

システムはデフォルトの認証ドメインを使用します。デフォルト認証ドメインの詳細は、オペレーションマニュアルのセクション 12 *ユーザアクセスと認証の “AAA”の* **domain default enable** コマンドを参照してください。

View

System view

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメインの名前を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別しません。

説明

mac-authentication domain コマンドはグローバルあるいは指定ポートで認証ドメインを指定します。

undo mac-authentication domain コマンドはデフォルトに戻します。

グローバルの認証ドメインは MAC アドレス認証が有効なすべてのポートに適用します。指定ポートの認証ドメインは指定ポートのみに適用します。異なるポートで異なる認証ドメインを指定することができます。

ポートは、以下の順番で MAC アドレス認証ユーザの認証ドメインを選択します。

1) ポートで指定された認証ドメインを指定します。
2) system view で指定されたグローバルの認証ドメインを指定します。
3) デフォルトの認証ドメインを指定します。

例

グローバルの MAC アドレス認証ドメインとしてドメイン domain1 を指定します。

<AP> system-view

[AP] mac-authentication domain domain1

GigabitEthernet 1/0/1 の MAC アドレス認証ドメインとしてドメイン aabbcc を指定します。

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] mac-authentication domain aabbcc

関連コマンド

- **display mac-authentication**
- **domain default enable**

5.1.6 mac-authentication max-user

Syntax

mac-authentication max-user *max-number*

undo mac-authentication max-user

デフォルト

4294967295

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

max-number: ポートの MAC アドレス認証のユーザが同時に接続可能な最大数を設定します。設定範囲は 1～4294967295 です。

説明

mac-authentication max-user コマンドはポートの MAC アドレス認証のユーザが同時に接続可能な最大数を設定します。

undo mac-authentication max-user コマンドはデフォルトに戻します。

システムリソースが乱用されることを防止するため、ポートで MAC アドレス認証ユーザが同時に接続する最大数を設定します。最大数に到達したとき、ポートで後続の MAC アドレス認証ユーザは拒否されます。

例

GigabitEthernet 1/0/1 の MAC アドレス認証のユーザが同時に接続可能な最大数を 32 に設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] mac-authentication max-user 32

関連コマンド

display mac-authentication

5.1.7 mac-authentication timer

Syntax

mac-authentication timer { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** }

デフォルト

offline detect timer は 300 秒、quiet timer は 60 秒、server timeout timer は 100 秒です。

View

System view

定義済みユーザロール

network-admin

パラメータ

offline-detect *offline-detect-value*: offline detect timer を設定します。設定範囲は 60～65535 秒です。

quiet *quiet-value*: quiet timer を設定します。設定範囲は 1～3600 秒です。

server-timeout *server-timeout-value*: server timeout timer を設定します。設定範囲は 100～300 秒です。

説明

mac-authentication timer コマンドは MAC アドレス認証のタイマを設定します。

undo mac-authentication timer コマンドはデフォルトに戻します。

MAC アドレス認証ユーザは以下のタイマを使用します。

- **Offline detect timer**—ユーザがアイドル状態であることを検出するために、装置がユーザからのトラフィックを待つ期間を設定します。ユーザの接続が期間内でアイドル状態になっている場合、装置はユーザをログアウトし、ユーザのアカウントを停止します。このタイマは MAC アドレス認証のオフライン状態の検出機能が有効である場合のみ有効です。
- **Quiet timer**—MAC アドレス認証に失敗したユーザが MAC アドレス認証を実行できるようになるまで、装置が待つ時間をタイマに設定します。Quiet タイムの間は、MAC アドレスからのパケットはすべて廃棄されます。この Quiet メカニズムは、認証が繰り返され、システムのパフォーマンスに影響を与えることを防ぎます。

- **Server timeout timer**—RADIUS サーバが使用不能であることを検出するために、装置が RADIUS サーバからの応答を待つ時間をタイマに設定します。MAC アドレス認証中にタイムアウトした場合、ユーザはネットワークにアクセスすることはできません。

例

server timeout timer を 150 秒に設定します。

<AP> system-view

[AP] mac-authentication timer server-timeout 150

関連コマンド

display mac-authentication

5.1.8 mac-authentication user-name-format

Syntax

mac-authentication user-name-format { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *string*] | **mac-address** [{ **with-hyphen** [**six-section** | **three-section**] | **without-hyphen** } **[lowercase** | **uppercase**]] }

undo mac-authentication user-name-format

デフォルト

MAC アドレス認証のユーザ名とパスワードとして各ユーザの MAC アドレスが使用されます。MAC アドレスは 16 進数で、ハイフンなし、小文字です。

View

System view

定義済みユーザロール

network-admin

パラメータ

fixed: すべての MAC アドレス認証ユーザの共有アカウントを使用します。

account *name*: 共有アカウントのユーザ名を指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。アットマーク（@）は指定できません。指定しない場合、デフォルトのユーザ名が適用されます。

password: 共有ユーザアカウントのパスワードを指定します。

cipher: 暗号テキストのパスワードを設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含むすべてのパスワードは、暗号テキストで保存されます。

string: パスワードを指定します。大文字、小文字を区別します。

- **simple** が指定された場合、設定範囲は 1～63 文字です。
- **cipher** が指定された場合、設定範囲は 1～117 文字です。
- **a**

mac-address: MAC アドレス認証ユーザの MAC ベースユーザアカウントを使用します。以下のパラメータを使用してユーザ名とパスワードの形式を指定することができます。

- with-hyphen: MAC アドレスにハイフンを含みます。たとえば、xx-xx-xx-xx-xx-xx です。
  - **six-section**: MAC アドレスを xx-xx-xx-xx-xx-xx または XX-XX-XX-XX-XX-XX のように 2 桁の 16 進数で 6 グループにハイフネーションします。
  - **three-section**: MAC アドレスを xxxx-xxxx-xxxx または XXXX-XXXX のように 4 桁の 16 進数で 3 グループにハイフネーションします。
- **without-hyphen**: MAC アドレスにハイフンを含みません。たとえば、xxxxxxxxxxxx です。
- **lowercase**: 小文字を指定します。
- **uppercase**: 大文字を指定します。

説明

mac-authentication user-name-format コマンドは MAC アドレス認証ユーザのユーザアカウントのタイプを設定します。

undo mac-authentication user-name-format コマンドはデフォルトに戻します。

MAC ベースのユーザアカウントを指定する場合、装置は、ユーザの MAC アドレス認証のユーザ名とパスワードとしてユーザの MAC アドレスを使用します。ユーザアカウントタイプは認証のセキュリティを高めます。しかし、認証サーバは、ユーザ名とパスワードとしてユーザの MAC アドレスを使用し、各ユーザのユーザアカウントを作成する必要があります。

共有ユーザアカウントを使用する場合、装置は、すべてのユーザの MAC アドレス認証を行うため指定されたユーザ名とパスワードを使用します。すべての MAC アドレスユーザは、認証用に 1 つのアカウントを使用するため、認証サーバで 1 つのアカウントのみを作成します。このユーザアカウントタイプは信頼されたネットワーク用に適しています。

例

MAC アドレス認証ユーザの共有アカウントを設定し、ユーザ名を abc、パスワードをプレーンテキストで xyz に設定します。

```
<AP> system-view
[AP] mac-authentication user-name-format fixed account abc password simple xyz
```

MAC アドレス認証ユーザの MAC ベースユーザアカウントを設定します。各 MAC アドレスはハイフンつき、大文字の 16 進数で設定します。

<AP> system-view

[AP] mac-authentication user-name-format mac-address with-hyphen uppercase

関連コマンド

display mac-authentication

5.1.9 reset mac-authentication statistics

Syntax

reset mac-authentication statistics [**interface** *interface-type interface-number*]

View

User view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: ポートのタイプと番号を指定します。指定しない場合、すべてのグローバルと指定したポートに関する MAC アドレス認証の統計情報を削除します。

説明

reset mac-authentication statistics コマンドは MAC アドレス認証の統計情報を削除します。

例

GigabitEthernet 1/0/1 の MAC アドレス認証の統計情報を削除します。

<AP> reset mac-authentication statistics interface gigabitethernet 1/0/1

関連コマンド

display mac-authentication

QX-W610 アクセスポイント

コマンドマニュアル

13. セキュリティ

本マニュアルは以下に示す章で構成されています。

01-ACL
02-タイムレンジ
03-ユーザプロファイル
04-公開鍵
05-SSH
06-パスワード管理

目次

このセクションのページは **13-x-x** です。

1 章 ACL 1-1
1.1 ACL 設定コマンド 1-1
1.1.1 acl 1-1
1.1.2 acl copy 1-3
1.1.3 description 1-4
1.1.4 display acl 1-6
1.1.5 packet-filter (interface view) 1-7
1.1.6 packet-filter (service template view) 1-9
1.1.7 reset acl counter 1-10
1.1.8 rule (IPv4 advanced ACL view) 1-11
1.1.9 rule (IPv4 basic ACL view) 1-18
1.1.10 rule (Layer 2 ACL view) 1-20
1.1.11 rule (WLAN client ACL view) 1-22
1.1.12 rule comment 1-23
1.1.13 step 1-24

1章 ACL

1.1 ACL設定コマンド

1.1.1 acl

Syntax

acl {**name** acl-name | **number** acl-number [**name** acl-nam**e**] [match-order {auto|config}] }

undo acl { **all** | name acl-name | **number** acl-number }

acl { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

undo acl { **all** | { **advanced** | **basic** } { *acl-number* | **name** *acl-name* } }

acl mac { *acl-number* | **name** *acl-name* } [**match-order** { **auto** | **config** }]

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

acl wlan client { *acl-number* | **name** *acl-name* }

undo acl wlan client { *acl-number* | **all** | **name** *acl-name* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

basic: 標準 ACL を指定します。

advanced: 拡張 ACL を指定します。

mac: L2 ACL を指定します。

wlan client: WLAN クライアントの ACL のタイプを指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 100～199：WLAN クライアントの ACL です。
- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *acl-name*: ACL を識別しやすくするため、ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

match-order: パケットを比較する ACL ルールの順番を設定します。

- **auto**: 深さ優先順序に従って ACL ルールを比較します。
- **config**: ルール ID の昇順に従って ACL ルールを比較します。小さいルール ID は優先度が高くなります。ACL ルールの順序を指定しない場合、デフォルトで **config** が適用されます。

all: すべての ACL を指定します。

説明

acl コマンドは ACL を作成し、ACL の view に移行します。すでに ACL が作成されている場合、その view に移行します。

undo acl コマンドは指定された、あるいはすべての ACL を削除します。

ルールが含まれていない ACL のみ、比較順序を変更することができます。

ACL のルールが一致順序を含む、あるいは以下の一致基準が有効である場合、一致するパケットはソフトウェアベースのパケット転送を行います。

- 送信元 IP アドレス、宛先 IP アドレス
- 送信元ポート、宛先ポート
- トランスポートレイヤプロトコル
- ICMP のメッセージタイプ、メッセージコード
- ロギング
- タイムレンジ

ソフトウェアベースのパケット転送は、転送エントリのため、コントロールプレーンにパケットを送信します。これは装置のパケット転送に影響します。

例

標準 IPv4 ACL 2000 を作成し、その view に移行します。

<AP> system-view

[AP] acl basic 2000

[AP-acl-ipv4-basic-2000]

ACL 名が flow の標準 IPv4 ACL を作成し、その view に移行します。

<AP> system-view

[AP] acl basic name flow

[AP-acl-ipv4-basic-flow]

拡張 IPv4 ACL 3000 を作成し、その view に移行します。

<AP> system-view

[AP] acl advanced 3000

[AP-acl-ipv4-adv-3000]

L2 ACL 4000 を作成し、その view に移行します。

<AP> system-view

[AP] acl mac 4000

[AP-acl-mac-4000]

ACL 名が flow の L2 ACL を作成し、その view に移行します。

<AP> system-view

[AP] acl mac name flow

[AP-acl-mac-flow]

ACL 名が 100 の WLAN クライアントの ACL を作成し、その view に移行します。

<AP> system-view

[AP] acl wlan client 100

[AP-acl-client-100]

ACL 名が flow の WLAN クライアントの ACL を作成し、その view に移行します。

<AP> system-view

[AP] acl wlan client name flow

[AP-acl-client-flow]

関連コマンド

display acl

1.1.2 acl copy

Syntax

acl [**mac**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

View

System view

定義済みユーザロール

network-admin

パラメータ

mac: L2 ACL を指定します。

source-acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 100～199：WLAN クライアントの ACL です。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

name *source-acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。

dest-acl-number: 新しい ACL の番号を指定します。以下に設定範囲を示します。

- 100～199：WLAN クライアントの ACL です。
- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。

name *dest-acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。最初の文字は英字を使用する必要があります。混乱を避けるため、**all** は使用できません。

説明

acl copy コマンドは既存の ACL をコピーします。

新しい ACL は既存の ACL と同一タイプにする必要があります。

新しい ACL は既存の ACL とカテゴリ、同一内容ですが、ACL 名と ACL 番号が異なります。

IPv4 ACL を指定する場合、**mac** パラメータを指定しないでください。

例

標準 IPv4 ACL 2001 をコピーし、標準 IPv4 ACL 2002 を作成します。

<AP> system-view

[AP] acl copy 2001 to 2002

ACL 名が test の標準 IPv4 ACL をコピーし、ACL 名が paste の標準 IPv4 ACL を作成します。

<AP> system-view

[AP] acl copy name test to name paste

1.1.3 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

IPv4 basic/advanced ACL view

Layer 2 ACL view

WLAN client ACL view

定義済みユーザロール

network-admin

パラメータ

text: ACL の説明を設定します。設定範囲は 1～127 です。大文字、小文字は区別します。

説明

description コマンドは ACL の説明を設定します。

undo description コマンドは ACL の説明を削除します。

例

標準 IPv4 ACL 2000 の説明を設定します。

<AP> system-view

[AP] acl basic 2000

[AP-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.

関連コマンド

display acl

1.1.4 display acl

Syntax

display acl [**mac** | **wlan**] { *acl-number* | **all** | **name** *acl-name* }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

mac: L2 ACL を指定します。

wlan: WLAN クライアントの ACL のタイプを指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 100～199：WLAN クライアントの ACL です。
- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

all: すべての ACL を指定します。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。

説明

display acl コマンドは ACL の設定と一致する統計情報を表示します。

ACL ルールの順番が設定されたとき、このコマンドは **config** あるいは **auto** で表示します。

IPv4 ACL を指定する場合、**mac** パラメータを指定しないでください。

例

全ての標準 IPv4 ACL の設定と一致する統計情報を表示します。

<AP> display acl all

```
Basic IPv4 ACL 2001, 2 rules, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used on GigabitEthernet 1/0/1.
Advanced IPv4 ACL 3001, 1 rule,
ACL's step is 5
```

```
rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255 (Dynamic)
```

表 1-1 コマンド出力

フィールド	説明
Basic IPv4 ACL 2001	ACLのカテゴリと番号です。フィールドの情報は標準IPv4 ACL 2001です。
2 rule	ACLは2つのルールがあることを示します。
match-order is auto	ACLの比較順序が**auto**です。深さ優先順序に従ってACLルールを比較します。比較順序が**config**である場合は表示されません。
This is an IPv4 basic ACL.	ACLの説明です。
ACL's step is 5	ルールのステップ数が5です。
rule 5 permit source 1.1.1.1 0	ルール5の内容です。IPアドレス1.1.1.1からのパケットを許可します。
5 times matched	ルールに5回一致しています。統計情報はソフトウェアで実行されたACLに一致した回数です。 ルールに一致していない場合、フィールドは表示されません。
rule 5 comment This rule is used on GigabitEthernet 1/0/1.	ACLルール5の説明です。
Dynamic	このルールは、モジュールにより動的に付加されます。

1.1.5 packet-filter (interface view)

Syntax

packet-filter [**mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

undo packet-filter [**mac**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

デフォルト

パケットをフィルタリングするためにインタフェースに ACL の適用は、なし。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

mac: レイヤ 2 ACL タイプを指定します。

acl-number: ACL を番号で指定します。使用可能な値の範囲は次のとおりです。

- basic ACL の場合は 2000 ～ 2999。
- advanced ACL の場合は 3000 ～ 3999。
- Layer 2 ACL の場合は 4000 ～ 4999。

name *acl-name*: ACL を名前で指定します。 acl-name 引数は、大文字と小文字を区別しない 1 ～ 63 文字の文字列です。

inbound: 受信パケットをフィルタリングします。

outbound: 送信パケットをフィルタリングします。

説明

packet-filter を使用してインタフェースに ACL を適用し、パケットをフィルタリングします。

undo packet-filter を使用して、インタフェースから ACL を削除します。

このコマンドは、aggregation group のメンバ ポートには効果がありません。

例

IPv4 basic ACL 2001 を適用して、GigabitEthernet 1/0/1 上の受信トラフィックをフィルタリングします。

```
<AP> system-view
[AP] interface gigabitethernet 1/0/1
[AP-GigabitEthernet1/0/1] packet-filter 2001 inbound
```

関連コマンド

display packet-filter

display packet-filter statistics

display packet-filter verbose

1.1.6 packet-filter (service template view)

Syntax

packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

undo packet-filter { **inbound** | **outbound** }

デフォルト

パケットをフィルタリングするためにサービス テンプレートに ACL の適用は、なし。

View

Service template view

定義済みユーザロール

network-admin

パラメータ

acl-number: ACL を番号で指定します。使用可能な値の範囲は次のとおりです。

- basic ACL の場合は 2000 ～ 2999。
- advanced ACL の場合は 3000 ～ 3999。

name *acl-name*: ACL を名前で指定します。 acl-name 引数は、大文字と小文字を区別しない 1 ～ 63 文字の文字列です。

inbound: 受信パケットをフィルタリングします。

outbound: 送信パケットをフィルタリングします。

説明

packet-filter を使用して、サービス テンプレートに ACL を適用し、パケットをフィルタします。

undo packet-filter を使用して、サービス テンプレートから ACL を削除します。

サービス テンプレートのパケットをフィルタリングするには、ACL を AC 上のサービス テンプレートに適用し、適用された ACL を AP 上に作成する必要があります。サービス テンプレートに適用される ACL は、パケットの送信元 IP アドレス、宛先 IP アドレス、送信元ポート番号、宛先ポート番号、およびプロトコルとのみ一致します。サービステンプレートの同じ方向に適用できる ACL は 1 つだけです。このコマンドはサービステンプレートが無効な場合のみ実行できます。

例

IPv4 basic ACL 2001 を適用して、サービス テンプレート service1 の受信トラフィックをフィルタリングします。

```
<AP> system-view
[AP] wlan service-template service1
[AP-wlan-st-service1] packet-filter 2001 inbound
```

1.1.7 reset acl counter

Syntax

reset acl [**mac**] **counter** { *acl-number* | **all** | **name** *acl-name* }

View

User view

定義済みユーザロール

network-admin

パラメータ

mac: L2 ACL を指定します。

acl-number: ACL の番号を指定します。以下に設定範囲を示します。

- 2000～2999：標準 ACL です。
- 3000～3999：拡張 ACL です。
- 4000～4999：L2 ACL です。**mac** の指定が必要です。

all: すべての ACL の統計情報を削除します。

name *acl-name*: ACL 名を指定します。設定範囲は 1～63 です。大文字、小文字は区別しません。

説明

reset acl counter コマンドは ACL の統計情報を削除します。

例

標準 IPv4 ACL 2001 の統計情報を削除します。

<AP> reset acl counter 2001

関連コマンド

display acl

1.1.8 rule (IPv4 advanced ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } ***** | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | *destination-port operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } ***** } | **fragment** | *icmp-type* { *icmp-type* [*icmp-code*] | *icmp-message* } | logging | **source** { *source-address source-wildcard* | *any* } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *****

undo rule rule-id [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } ***** | **established** } | **counting | destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } ***** } | **fragment** | **icmp-type** | **logging | source** | **source-port** | **time-range**] *****

undo rule [rule-id] { **deny** | **permit** } protocol [{ { **ack** ack-value | fin fin-value | **psh** psh-value | **rst** rst-value | **syn** syn-value | **urg** urg-value } * | **established** } | **counting** | **destination** { dest-address dest-wildcard | **any** } | **destination-port** operator port1 [port2] | { **dscp** dscp | { **precedence** precedence | tos tos } * } | fragment | icmp-type { icmp-type [icmp-code] | icmp-message } | **logging** | **source**{ source-address source-wildcard | **any** } | **source-port** operator port1 [port2] | **time-range** time-range-name]

デフォルト

設定なし

View

IPv4 advanced ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

protocol: プロトコル番号あるいはプロトコル名を指定します。

- プロトコル番号の設定範囲は 0～255 です。
- プロトコル名は **gre** (47)、**icmp** (1)、**igmp** (2)、**ip**、**ipinip** (4)、**ospf** (89)、**tcp** (6)、**udp** (17)を指定できます。**ip** はすべてのプロトコルを指定します。表 1-2 にプロトコルの値に関わらず指定できるパラメータを示します。

表 1-2 拡張 IPv4 ACL ルールの一致基準と他のルールの情報

パラメータ	機能	説明
source { *source-address* *source-wildcard* | **any** }	送信元アドレスを定義します。	*source-address*と*source-wildcard*はドットで区切られた10進数表記の送信元IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。**any**は、任意の送信元IPアドレスを示します。
destination { *dest-address* *dest-wildcard* | **any** }	宛先アドレスを定義します。	*dest-address*と*dest-wildcard*はドットで区切られた10進数表記の宛先IPアドレスとワイルドカードマスクを示します。すべてが0のワイルドカードはホストアドレスを示します。**any**は、任意の宛先IPアドレスを示します。
counting	ソフトウェアでルールー致カウントを有効にします。	countingのキーワードは、ルールに固有の一致カウントを有効にします。countingのキーワードが指定されていない場合、ルールの一致はソフトウェアでカウントされません。
precedence *precedence*	IPプレシーデンスの値を指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～7です。名前は**routine** (0)、**priority** (1)、**immediate** (2)、**flash** (3)、**flash-override** (4)、**critical** (5)、**internet** (6)、**network** (7)が指定できます。
tos *tos*	ToSプレシーデンスを指定します。	プレシーデンスの値あるいはプレシーデンスの名前を指定します。番号の設定範囲は0～15です。名前は**max-reliability** (2)、**max-throughput** (4)、**min-delay** (8)、**min-monetary-cost** (1)、**normal** (0)が指定できます。
dscp dscp	DSCPプライオリティを指定します。	*dscp*プライオリティの値あるいはプライオリティの名前を指定します。番号の設定範囲は0～63です。名前は**af11** (10)、**af12** (12)、**af13** (14)、**af21** (18)、**af22** (20)、**af23** (22)、**af31** (26)、**af32** (28)、**af33** (30)、**af41** (34)、**af42** (36)、**af43** (38)、**cs1** (8)、**cs2** (16)、**cs3** (24)、**cs4** (32)、**cs5** (40)、**cs6** (48)、**cs7** (56)、**default** (0)、**ef** (46)が指定できます。

パラメータ	機能	説明
fragment	最初のフラグメントではないフラグメントを指定します。	指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。
logging	一致するパケットの数をログに記録します。	この機能では、ACL を使用するモジュール (パケット フィルタリングなど) がロギングをサポートしている必要があります。
time-range *time-range-name*	ルールのタイムレンジを指定します。	*time-range-name*の設定範囲は1～32文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション13 *セキュリティ "タイムレンジ"*を参照してください。

*protocol*が**tcp** (6)あるいは**udp** (7)である場合、設定するパラメータを表 1-3に示します。

表 1-3 拡張 IPv4 ACL ルールの TCP/UDP 指定パラメータ

パラメータ	機能	説明
source-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの送信元ポート番号を指定します。	*operator*は**lt** (lower than)、**gt** (greater than)、**eq** (equal to)、**neq** (not equal to)、**range** (inclusive range)が指定できます。*port1*、*port2*はTCPあるいはUDPポート番号です。設定範囲は0～65535です。*port2*

パラメータ	機能	説明
destination-port *operator port1* [*port2*]	1つまたは複数のTCP/UDPの宛先ポート番号を指定します。	は*operator*が範囲であるときのみ必要です。TCPポート番号は以下の名前で指定できます。**chargen** (19)、**bgp** (179)、**cmd** (514)、**daytime** (13)、**discard** (9)、**domain** (53)、**echo** (7)、**exec** (512)、**finger** (79)、**ftp** (21)、**ftp-data** (20)、**gopher** (70)、**hostname** (101)、**irc** (194)、**klogin** (543)、**kshell** (544)、**login** (513)、**lpd** (515)、**nntp** (119)、**pop2** (109)、**pop3** (110)、**smtp** (25)、**sunrpc** (111)、**tacacs** (49)、**talk** (517)、**telnet** (23)、**time** (37)、**uucp** (540)、**whois** (43)、**www** (80) UDPポート番号は以下の名前で指定できます **biff** (512)、**bootpc** (68)、**bootps** (67)、**discard** (9)、**dns** (53)、**dnsix** (90)、**echo** (7)、**mobilip-ag** (434)、**mobilip-mn** (435)、**nameserver** (42)、**netbios-dgm** (138)、**netbios-ns** (137)、**netbios-ssn** (139)、**ntp** (123)、**rip** (520)、**snmp** (161)、**snmptrap** (162)、**sunrpc** (111)、**syslog** (514)、**tacacs-ds** (65)、**talk** (517)、**tftp** (69)、**time** (37)、**who** (513)、**xdmcp** (177)
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	ACK、FIN、PSH、RST、SYN、URGを含む1つまたは複数のTCPフラグを指定します。	TCP用のパラメータです。各値は0(フラグビットがセットされていません)または1(フラグビットがセットされています)が指定できます。ルールのTCPフラグはANDの関係です。たとえば、ack 0 psh 1が設定されたルールはACKフラグが設定されておらず、PSHフラグが設定されているパケットに一致します。
established	TCP接続の確立状態を示すフラグを指定します。	TCP用のパラメータです。ルールはACKあるいはRSTフラグがセットされているTCP接続パケットに一致します。

protocol が **icmp** (1)である場合、設定するパラメータを表 1-4 に示します。

表 1-4 拡張 IPv4 ACL ルールの ICMP 指定パラメータ

パラメータ	機能	説明
icmp-type { **icmp-type** *icmp-code* | *icmp-message* }	ICMPメッセージタイプとコードを指定します。	*icmp-type*の設定範囲は0～255です。*icmp-code*の設定範囲は0～255です。*icmp-message*はメッセージの名前を指定します。サポートされるICMPメッセージ名と対応するタイプとコードの値を表 1-5に示します。

表 1-5 拡張 IPv4 ACL ルールでサポートされる ICMP メッセージ名

ICMP メッセージ名	ICMP メッセージタイプ	ICMP メッセージコード
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

説明

rule コマンドは拡張 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは拡張 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。その ACL に手入力で加えられたもう一つのルールと同一の **deny** あるいは **permit** がある ACL のルールの場合、そのルールは作成あるいは修正することができません。その ACL に動的に加えられたルールと同一の **deny** あるいは **permit** がある ACL のルールの場合、そのルールは動的に加えられたルールを上書きします。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

標準 IPv4 ACL、拡張 IPv4 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

例

アドレス 129.9.0.0/16 から 202.38.160.0/24 の宛先ポート 80 の TCP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AP> system-view

[AP] acl advanced 3000

[AP-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80

192.168.1.0/24 宛の ICMP パケットを除くすべての IP パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AP> system-view

[AP] acl advanced 3001

[AP-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255

[AP-acl-ipv4-adv-3001] rule permit ip

FTP の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AP> system-view

[AP] acl advanced 3002

[AP-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp

[AP-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data

[AP-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp

[AP-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data

SNMP と SNMP trap の送受信パケットを許可する拡張 IPv4 ACL ルールを作成します。

<AP> system-view

[AP] acl advanced 3003

[AP-acl-ipv4-adv-3003] rule permit udp source-port eq snmp

[AP-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap

[AP-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp

[AP-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range**

1.1.9 rule (IPv4 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [counting | **fragment** | **source**

{ *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **fragment** | logging | **source** | **time-range**] *

undo rule [rule-id] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source**

{ source-address source-wildcard | any } | time-range time-range-name] *

デフォルト

設定なし

View

IPv4 basic ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

counting: ソフトウェアでルール一致カウントを有効にします。このキーワードを指定しない場合、ルールの一致はソフトウェアでカウントされません。

fragment: 最初のフラグメントではないフラグメントを指定します。指定しない場合、ルールはすべてのフラグメントと非フラグメントを適用します。

logging: 一致するパケットの数をログに記録します。この機能は、ACL を使用するアプリケーション モジュール (パケット フィルタリングなど) がロギング機能をサポートしている場合にのみ使用できます。

source { *source-address source-wildcard* | **any** }: 送信元アドレスを定義します。*source-address* と *source-wildcard* はドットで区切られた 10 進数表記の送信元 IP アドレスとワイルドカードマスクを示します。すべてが 0 のワイルドカードはホストアドレスを示します。**any** は、任意の送信元 IP アドレスを示します。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用

する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 13 *セキュリティ “タイムレンジ”* を参照してください。

説明

rule コマンドは標準 IPv4 ACL のルールを作成あるいは修正します。

undo rule コマンドは標準 IPv4 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

標準 IPv4 ACL、拡張 IPv4 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

例

アドレス 10.0.0.0/8、172.17.0.0/16、192.168.1.0/24 を除く送信元 IP セグメントからのパケットを拒否する標準 IPv4 ACL ルールを作成します。

<AP> system-view

[AP] acl basic 2000

[AP-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255

[AP-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255

[AP-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255

[AP-acl-ipv4-basic-2000] rule deny source any

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range**

1.1.10 rule (Layer 2 ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | counting | **dest-mac**
dest-address dest-mask | { **lsap** *lsap-type lsap-type-mask* | **type**
protocol-type protocol-type-mask } | **source-mac** *source-address*
source-mask | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **time-range**]

undo rule [rule-id] { **deny** | **permit** } [**cos** dot1p | **counting** | **dest-mac**
dest-address dest-mask | { **lsap** lsap-type lsap-type-mask | **type**
protocol-type protocol-type-mask } | **source-mac** source-address
source-mask | **time-range** time-range-name] *

デフォルト

設定なし

View

Layer 2 ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

cos *dot1p*: 802.1p プライオリティを定義します。

- プライオリティの設定範囲は 0～7 です。
- **best-effort** (0)、**background** (1)、**spare** (2)、**excellent-effort** (3)、**controlled-load** (4)、**video** (5)、**voice** (6)、**network-management** (7)の用語で定義することができます。

counting: ソフトウェアでルール一致カウントを有効にします。

このキーワードを指定しない場合、ルールの一致はソフトウェアでカウントされません。

dest-mac *dest-address dest-mask*: 宛先 MAC アドレス範囲を定義します。*dest-address* と *dest-mask* は宛先 MAC アドレスとマスクを示します。マスクの形式は H-H-H です。

lsap *lsap-type lsap-type-mask*: LLC カプセル化の DSAP と SSAP フィールドを定義します。*lsap-type* は 16 進数表記でカプセル化フォーマットを示します。*lsap-type* の設定範囲は 0～ffff です。*lsap-type-mask* は 16 進数表記で LSAP マスクを示します。*lsap-type-mask* の設定範囲は 0～ffff です。

type *protocol-type protocol-type-mask*: L2 の 1 つ以上のプロトコルを定義します。*protocol-type* は 16 進数表記で Ethernet_II と Ethernet_SNAP のプロトコルタイプを示します。*protocol-type* の設定範囲は 0～ffff です。*protocol-type-mask* は 16 進数表記でプロトコルタイプのマスクを示します。*protocol-type-mask* の設定範囲は 0～ffff です。

source-mac *source-address source-mask*: 送信元 MAC アドレス範囲を定義します。*source-address* は送信元 MAC アドレスを示します。*sour-mask* はマスクを示します。マスクの形式は H-H-H です。

time-range *time-range-name*: ルールのタイムレンジを指定します。*time-range-name* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。最初の文字は英字を使用する必要があります。タイムレンジが設定されていない場合、システムはルールを作成しますが、タイムレンジを設定した後、タイムレンジを使用したルールが適用されます。タイムレンジの詳細は、オペレーションマニュアルのセクション 13 *セキュリティ “タイムレンジ”* を参照してください。

説明

rule コマンドは L2 ACL のルールを作成あるいは修正します。

undo rule コマンドは L2 ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

一致の順番が **config** であるときのみ ACL ルールを修正することができます。

L2 ACL のルールとルールの ID を表示する場合、**display acl all** コマンドを使用します。

すべてのパラメータを指定しない場合、**undo rule** *rule-id* コマンドはすべてのルールを削除します。パラメータを指定した場合、**undo rule** *rule-id* コマンドは指定した属性を削除します。

例

L2 ACL 4000 のルールを作成します。ARP パケットを許可し、RARP パケットを拒否します。

<AP> system-view

[AP] acl mac 4000

[AP-acl-mac-4000] rule permit type 0806 ffff

[AP-acl-mac-4000] rule deny type 8035 ffff

関連コマンド

- **acl**
- **display acl**
- **step**
- **time-range**

1.1.11 rule (WLAN client ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**ssid** *ssid-name*]

undo rule *rule-id*

デフォルト

設定なし

View

WLAN client ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ルール ID を指定します。設定範囲は 0～65534 です。ACL ルールを作成するとき、ルール ID を指定しない場合、システムは自動でルール ID を割り当てます。0 から始まり現在のもっとも大きいルール ID より大きなステップの最小倍数をルールに割り当てます。たとえば、ステップが 5 のときに、現在のもっとも大きいルール ID が 28 の場合、ルールに 30 の番号を割り当てます。

deny: 一致するパケットを拒否します。

permit: 一致するパケットを許可します。

ssid *ssid-name*: その名前を SSID に設定します。設定範囲は 1～32 文字です。大文字、小文字を区別しません。この設定を行わない場合、自動的に適当な SSID が適用されます。

説明

rule コマンドは WLAN クライアント ACL のルールを作成あるいは修正します。

undo rule コマンドは WLAN クライアント ACL ルールを削除あるいはルールから属性を削除します。

ACL で各ルールの **permit** あるいは **deny** は固有にする必要があります。別のルールと同一の **deny** あるいは **permit** がある ACL のルールを作成あるいは修正する場合、ルールは作成あるいは修正することができません。

WLAN クライアント ACL のルールを表示する場合、**display acl wlan all** コマンドを使用します。

例

WLAN クライアント ACL 111 のルールを作成します。permit パケットの SSID は ME、deny パケットの SSID は HIM とします。

<AP> system-view

[AP] acl wlan client 111

[AP-acl-client-111] rule permit ssid ME

[AP-acl-client-111] rule deny ssid HIM

関連コマンド

- **acl wlan client**
- **display acl**
- **step**

1.1.12 rule comment

Syntax

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

デフォルト

設定なし

View

IPv4 basic/advanced ACL view

Layer 2 ACL view

WLAN client ACL view

定義済みユーザロール

network-admin

パラメータ

rule-id: ACL のルール ID を指定します。設定範囲は 0～65534 です。ACL のルールはすでに作成されている必要があります。

text: ACL のルールの説明を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

rule comment コマンドは ACL のルールの説明を設定します。

undo rule comment コマンドは ACL のルールの説明を削除します。

ルールに説明がない場合、ルールに説明を追加します。すでにルールに説明がある場合、ルールの説明を修正します。

例

標準 IPv4 ACL 2000 を作成し、ルールの説明を追加します。

<AP> system-view

[AP] acl basic 2000

[AP-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0

[AP-acl-ipv4-basic-2000] rule 0 comment This rule is used on gigabitethernet 1/0/1.

関連コマンド

display acl

1.1.13 step

Syntax

step *step-value*

undo step

デフォルト

5

View

IPv4 basic/advanced ACL view

Layer 2 ACL view

WLAN client ACL view

定義済みユーザロール

network-admin

パラメータ

step-value: ACL ルールのステップ数を指定します。設定範囲は 1〜20 です。

説明

step コマンドは ACL ルールに自動的に番号を割り振るためのステップ数を設定します。

undo step コマンドはデフォルトに戻します。

ルールの番号づけステップはシステムが自動的にルール番号の増分を設定します。たとえば、デフォルトの ACL の番号づけステップは 5 です。ルールを作成するとき、ID を割り当てない場合、ルールの番号は 0、5、10、15...と番号づけられます。番号づけのステップを広くする場合、2 つのルールの間に多くのルールを挿入することができます。ステップを変更したときはいつでも、ルールは 0 から再ナンバリングが行われます。たとえば、5 つのルールの番号 5、10、13、15、20 がつけられている場合、ステップを 5 から 2 に変更すると、ルールの番号は 0、2、4、6、8 に再ナンバリングされます。

例

標準 IPv4 ACL 2000 のステップ数を 2 に設定します。

<AP> system-view

[AP] acl basic 2000

[AP-acl-ipv4-basic-2000] step 2

関連コマンド

display acl

目次

このセクションのページは **13-x-x** です。

2 章 タイムレンジ..... 2-1
2.1 タイムレンジ設定コマンド..... 2-1
2.1.1 display time-range..... 2-1
2.1.2 time-range..... 2-3

2章 タイムレンジ

2.1 タイムレンジ設定コマンド

2.1.1 display time-range

Syntax

display time-range { *time-range-name* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

time-range-name: タイムレンジの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別しません。

all: 既存のすべてのタイムレンジの設定と状態を表示します。

説明

display time-range コマンドはタイムレンジの設定と状態を表示します。

例

タイムレンジ t4 の設定と状態を表示します。

```
<AP> display time-range t4
Current time is 17:12:34 11/23/2010 Tuesday

Time-range : t4 (Inactive)
10:00 to 12:00 Mon
14:00 to 16:00 Wed
from 00:00:00 1/1/2011 to 00:00:00 1/1/2012
from 00:00:00 6/1/2011 to 00:00:00 7/1/2011
```

すべてのタイムレンジの設定とステータスを表示します。

```
<AP> display time-range all
Current time is 17:23:41 6/28/2021 Monday

Time-range: aa (Inactive)
Yundi Alias:AA Tenant: aa
Monthly 12:00 1st to 13:00 11th
from 00:00:00 6/28/2021 to 00:00:00 31/12/2021

Time-range: ee (Inactive)
Yundi Alias:BBB Tenant: bb
Description:aaa

Time-range: bb (Inactive)
Yundi Alias:BB Tenant: bb
Weekly 13:00 Mon to 13:11 Fri
from 00:00:00 6/28/2021 to 00:00:00 31/12/2021
```

表 2-1 コマンド出力

フィールド	説明
Current time	現在のシステム時間です。
Time-range	タイムレンジの設定と状態です。タイムレンジ名、状態（activeあるいはinactive）、開始時間、終了時間が含まれます。
Alias	タイムレンジのAlias

2.1.2 time-range

Syntax

time-range *time-range-name* { { **monthly** | **weekly** } *start-day start-time* **to** *end-day end-time* [**from** *time1 date1*] [**to** *time2 date2*] | start-time **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [{ **monthly** | **weekly** } *start-day start-time* **to** *end-day end-time* [**from** *time1 date1*] [**to** *time2 date2*] | *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

time-range-name: タイムレンジの名前を指定します。設定範囲は 1〜32 文字です。大文字、小文字を区別しません。混乱をさけるため **all** を使用してはいけません。

monthly *start-day start-time* **to** *end-day end-time*: 月単位の時間範囲ステートメントを指定します。*start-day* 引数は開始日であり、*end-day* 引数は終了日です。start-day 引数と end-day 引数の値の範囲は、どちらも 1 ～ 31 です。終了日を開始日よりも小さくすることはできません。start-time と end-time はどちらも hh:mm または hh:mm:ss 形式 (24 時間制) です。start-time と end-time の値の範囲は両方とも 00:00:00 から 24:00:00 です。開始日と終了日が同じ日の場合、終了時刻は開始時刻よりも後である必要があります。

weekly *start-day start-time* **to** *end-day end-time*: 週単位の時間範囲ステートメントを指定します。*start-day* 引数は開始曜日であり、*end-day* 引数は終了曜日です。

- 日曜、月曜、火曜、水曜、木曜、金曜、土曜を表す 0 から 6 の範囲の数字。
- 曜日の略称：Sun、Mon、Tue、Wed、Thu、Fri、Sat。
- 終了日を開始日よりも小さくすることはできません。
- *start-time* と *end-time* はどちらも hh:mm または hh:mm:ss 形式 (24 時間制) です。*start-time* と *end-time* の値の範囲は両方とも 00:00:00 から 24:00:00 です。開始曜日と終了曜日が同じ場合、終了時刻は開始時刻よりも後である必要があります。

start-time **to** *end-time*: 周期的なタイムレンジを指定します。*start-time* と *end-time* の形式は hh:mm です。24 時間時計です。*start-time* の設定範囲は 00:00～23:59 です。*end-time* の設定範囲は 00:00～24:00 です。*end-time* は *start-time* よりも大きい値にする必要があります。

start-time **to** *end-time*: 毎日の時間範囲ステートメントを指定します。*start-time* と *end-time* はどちらも hh:mm または hh:mm:ss 形式 (24 時間制) です。開始時刻は 00:00:00 から 23:59:59、終了時刻は 00:00:00 から 24:00:00 の範囲の値です。終了時刻は開始時刻よりも大きくする必要があります。

days: 周期的なタイムレンジの日時あるいは曜日を指定します。複数の値を指定する場合、スペースで区切ります。値は重複することができません。値は以下のいずれかを指定することができます。

- 0～6：それぞれ日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日の設定範囲を指定します。
- **Sun**、**Mon**、**Tue**、**Wed**、**Thu**、**Fri**、**Sat**：曜日を指定します。
- **working-day**：月曜日～金曜日の営業日を指定します。
- **off-day**：土曜日、日曜日の非営業日を指定します。
- **daily**：一週間の日付を指定します。

from *time1 date1*: 絶対的なタイムレンジの開始時間と開始日を指定します。*time1* は時間を指定します。形式は hh:mm です。24 時間時計です。設定範囲は 00:00～23:59 です。*date1* は日付を指定します。形式は MM/DD/YYYY あるいは YYYY/MM/DD です。MM は 1～12 の月、*DD* は各月の日付、*YYYY* は 1970～2100 の年です。このパラメータを指定しない場合、開始時間と開始日はシステムで有効なもっとも早い時間の 01/01/1970 00:00 AM となります。

to *time2 date2*: 絶対的なタイムレンジの終了時間と終了日を指定します。*time2* は時間を指定します。形式は hh:mm です。24 時間時計です。設定範囲は 00:00～24:00 です。*date2* は日付を指定します。形式は MM/DD/YYYY あるいは YYYY/MM/DD です。MM は 1～12 の月、*DD* は各月の日付、*YYYY* は 1970～2100 の年です。このパラメータを指定しない場合、終了時間と終了日はシステムで有効なもっとも遅い時間の 12/31/2100 24:00 PM となります。

説明

time-range コマンドはタイムレンジを作成あるいは修正します。

undo time-range コマンドはタイムレンジあるいはタイムレンジのパラメータを削除します。

タイムレンジ名が既に存在する場合、タイムレンジのパラメータを追加します。

タイムレンジの複数のパラメータを作成することができます。各時間のパラメータは以下の形式の 1 つを指定することができます。

- *start-time* **to** *end-time days* の形式の周期的なパラメータを指定します。周期的なパラメータは日付あるいは曜日を周期的に繰り返します。
- *from time1 date1* **to** *time2 date2* の形式の絶対的なパラメータを指定します。一度限りで繰り返しません。

- *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* の形式の組み合わせを指定します。指定した期間内で日付あるいは曜日を周期的に繰り返します。たとえば、2015 年 1 月 1 日～12 月 31 日の月曜日の 8:00～12:00 の営業時間のタイムレンジ test を指定する場合、**time-range test 08:00 to 12:00 mon from 00:00 01/01/2015 to 23:59 12/31/2015** コマンドを使用します。

周期的なパラメータを最大 32、絶対的なパラメータを最大 12 の、最大 1024 のタイムレンジを作成することができます。タイムレンジのアクティブな期間を以下のように計算します。

1) すべての周期的なタイムレンジを組み合わせます。
2) すべての絶対的なタイムレンジを組み合わせます。
3) タイムレンジのアクティブな期間として 2 つの記述の AND を行います。

例

周期的なタイムレンジ t1 を作成し、営業時間の 8:00～18:00 をアクティブな期間に設定します。

<AP> system-view

[AP] time-range t1 08:00 to 18:00 working-day

絶対的なタイムレンジ t2 を作成し、2011 年のすべてをアクティブな期間に設定します。

<AP> system-view

[AP] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011

組み合わせのタイムレンジ t3 を作成し、2011 年の土曜日と日曜日の 8:00～12:00 をアクティブな期間に設定します。

<AP> system-view

[AP] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011

組み合わせのタイムレンジ t4 を作成し、2011 年の 1 月～6 月の月曜日の 10:00～12:00 と水曜日の 14:00～16:00 をアクティブな期間に設定します。

<AP> system-view

[AP] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011

[AP] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011

絶対的なタイムレンジ t5 を作成し、2018 年 1 月 1 日の 8:00 to 18:00 をアクティブな期間に設定します。

<AP> system-view

[AP] time-range t5 from 08:00:00 1/1/2018 to 18:00:00 1/1/2018

タイムレンジ t6 を作成し, 2021 年 1 月 1 日の 08:00 から 2021 年 12 月 1 日の 18:00 の間、月曜日の 08:00 から金曜日の 18:00 をアクティブにします。

<AP> system-view

[AP] time-range t6 weekly 1 08:00 to 5 18:00 from 08:00 1/1/2021 to 18:00 1/12/2021

関連コマンド

display time-range

目次

このセクションのページは **13-x-x** です。

3 章 ユーザプロファイル 3-1
3.1 ユーザプロファイル設定コマンド 3-1
3.1.1 display user-profile 3-1
3.1.2 user-profile 3-3

3章 ユーザプロファイル

3.1 ユーザプロファイル設定コマンド

3.1.1 display user-profile

Syntax

display user-profile [name *profile-name* **]**

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

name *profile-name*: ユーザプロファイル名を指定します。設定範囲は 1 から 31 文字です。大文字と小文字を区別します。英字、数字、アンダースコア (_) を使用可能です。名前は英字で始まり、一意である必要があります。このオプションを指定しない場合、すべてのユーザプロファイルの設定およびオンラインユーザ情報が表示されます。

説明

display user-profile コマンドはユーザプロファイルの設定およびオンラインユーザ情報を表示します。

例

#ユーザプロファイル aaa の設定とオンラインユーザ情報を表示します。

```
<AP> display user-profile name aaa
    User-Profile: aaa
     Inbound:
         Committed Access Rate:
             Rule: If-match any
                 CIR 64 (kbps), CBS 512 (Bytes), EBS 0 (Bytes), PIR 888 (kbps)
             Rule: If-match acl 2000
                 CIR 3000 (kbps), CBS 187500 (Bytes), EBS 0 (Bytes)
         Policy: p1
     Outbound:
```

Committed Access Rate:

Rule: If-match acl 3000

CIR 1000 (kbps), CBS 62500 (Bytes), EBS 0 (Bytes)

Rule: If-match any

CIR 64 (kbps), CBS 512 (Bytes), EBS 0 (Bytes), PIR 888 (kbps)

User user_1:

Authentication type: Portal

Network attributes:

Interface : GigabitEthernet1/0/1

MAC address : 0000-1111-2222

Failed action list:

Inbound: Policy p1

Inbound: CIR 64 (kbps), CBS 2048 (Bytes), EBS 0 (Bytes), PIR 888 (kbps)

表 3-1 コマンド出力

フィールド	説明
User-Profile	ユーザプロファイル名です。
Inbound	受信トラフィックに適用されるポリシーです。
Outbound	送信トラフィックに適用されるポリシーです。
Session-Group-Profile	セッショングループのプロファイル名です。
CIR	適用されるCIRを表示します。 コミットされた情報レート (kbps単位)。
CBS	適用されるCBSを表示します。 コミットされたバースト サイズ (バイト単位)。
EBS	適用されるEBSを表示します。 超過バースト サイズ (バイト単位)。
PIR	適用されるPIRを表示します。 ピーク情報レート(kbps単位)。
Policy	ポリシー名です。
User user_1	ユーザプロファイルが関連付けられているユーザアカウントのユーザ名です。
Authentication type	認証の種類です。 · 802.1X–802.1X認証です。 · Portal–ポータル認証です。 · PPP–PPP認証です。

フィールド	説明
Network attributes	オンラインユーザ情報です。
Failed action list	ユーザに適用できなかったアクションです。
Rule	一致したルール

3.1.2 user-profile

Syntax

user-profile *profile-name*

undo user-profile *profile-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

profile-name: ユーザプロファイル名を指定します。設定範囲は 1 から 31 文字です。大文字と小文字を区別します。英字、数字、アンダースコア (_) を使用でき、英字で始まる必要があります。名前は一意である必要があります。

説明

user-profile コマンドはユーザプロファイルを作成し、その view に移行するか、既存のユーザプロファイルの view に移行します。

undo user-profile コマンドはユーザプロファイルを削除します。

例

#ユーザプロファイル a123 を作成し、a123 の View に移行します。

<AP> system view

[AP] user-profile name a123

[AP-user-profile-a123]

目次

このセクションのページは **13-x-x** です。

4 章 公開鍵 4-1
4.1 公開鍵設定コマンド 4-1
4.1.1 display public-key local public 4-1
4.1.2 display public-key peer 4-5
4.1.3 peer-public-key end 4-7
4.1.4 public-key local create 4-8
4.1.5 public-key local destroy 4-13
4.1.6 public-key local export dsa 4-15
4.1.7 public-key local export rsa 4-17
4.1.8 public-key peer 4-20
4.1.9 public-key peer import sshkey 4-22

4章 公開鍵

4.1 公開鍵設定コマンド

4.1.1 display public-key local public

Syntax

display public-key local { **dsa** | **ecdsa** | **rsa** } **public** [**name** *key-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

dsa: DSA 鍵ペアタイプを指定します。

ecdsa: ECDSA 鍵ペアタイプを指定します。

rsa: RSA 鍵ペアタイプを指定します。

name *key-name*: ローカル非対称鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を指定しない場合、指定されたタイプのすべてのローカル非対称鍵ペアの公開鍵を表示します。

説明

display public-key local public コマンドはローカル鍵ペアを表示します。

例

すべてのローカル RSA 鍵ペアの公開鍵を表示します。

<AP> display public-key local rsa public

```
=============================================
Key name: hostkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
   30819F300D06092A864886F70D010101050003818D0030818902818100DAA4AAFEFE04C2C9
   667269BB8226E26331E30F41A8FF922C7338208097E84332610632B49F75DABF6D871B80CE
   C1BA2B75020077C74745C933E2F390DC0B39D35B88283D700A163BB309B19F8F87216A44AB
```

```
  FBF6A3D64DEB33E5CEBF2BCF26296778A26A84F4F4C5DBF8B656ACFA62CD96863474899BC1
  2DA4C04EF5AE0835090203010001
=============================================
Key name: serverkey (default)
Key type: RSA
Time when key pair created: 15:40:48 2011/05/12
Key code:
  307C300D06092A864886F70D0101010500036B003068026100CAB4CACCA16442AD5F453442
  762F03897E0D494FEDE69224F5C051A441D290976733A278C9F0C0F5A198E66143EAB54A64
  DB608269CAE844B1E7CC64AD7E808972E7CF887F3B657F056E7930FC84FBF1AD83A01CC47E
  9D85C13413996ECD093B0203010001
=============================================
Key name: rsa1
Key type: RSA
Time when key pair created: 15:42:26 2011/05/12
Key code:
  30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
  426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
  1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
  9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
  92D8C6D940890BF4290203010001
```

すべてのローカル DSA 鍵ペアの公開鍵を表示します。

<AP> display public-key local dsa public

```
=============================================
Key name: dsakey (default)
Key type: DSA
Time when key pair created: 15:41:37 2011/05/12
Key code:
  308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
  96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
  DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
  DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
  7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
  4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
  35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
  91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
  585DA7F42519718CC9B09EEF038184000281804191 2CE34D12BCD2157E7AB1C2F03B3EF395
  100F3DB4A9E2FDFE860C1BD663D676438F7DA40A9406D61CA9079AF13E330489F1C76785DE
  52DA649AC8BC04B6D39CD7C52CD0A14F75F7491A91D31D6AC22340B5981B27A915CDEC4F09
  887E541EC1E5302D500F68E7AC29A084463C60F9EE266985A502FC92193E1CF4D265C4BA
=============================================
```

```
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
   308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
   96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
   DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
   DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
   7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
   4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
   35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
   91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
   585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
   3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
   0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
   15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

ローカル ECDSA 鍵ペアの公開鍵を表示します。

<AP> display public-key local ecdsa public

```
=============================================
Key name: ecdsakey (default)
Key type: ECDSA
Key length: 192
Time when key pair created: 15:42:04 2011/05/12
Key code:
3049301306072A8648CE3D020106082A8648CE3D03010103320004C10CF7CE42193F7FC2AF
68F5DC877835A43009DB6135558A7FB8316C361B0690B4FD84A14C0779C76DD6145BF9362B
1D
=============================================
Key name: ecdsa1
Key type: ECDSA
Key length: 192
Time when key pair created: 15:43:33 2011/05/12
Key code:
3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
4D
```

ローカル RSA 鍵ペア **rsa1** の公開鍵を表示します。

<AP> display public-key local rsa public name rsa1

```
=============================================
```

```
Key name: rsa1
Key type: RSA
Key length: 1024
Time when key pair created: 15:42:26 2011/05/12
Key code:
30819F300D06092A864886F70D010101050003818D0030818902818100DEBC46F217DDF11D
426E7095AA45CD6BF1F87343D952569AC223A01365E0D8C91D49D347C143C5D8FAADA896AA
1A827E580F2502F1926F52197230E1DE391A64015C43DD79DC4E9E171BAEA1DEB4C71DAED7
9A6EDFD460D8945D27D39B7C9822D56AEA5B7C2CCFF1B6BC524AD498C3B87D4BD6EB36AF03
92D8C6D940890BF4290203010001
```

ローカル DSA 鍵ペア dsa1 の公開鍵を表示します。

<AP> display public-key local dsa public name dsa1

```
==========================================
Key name: dsa1
Key type: DSA
Time when key pair created: 15:35:42 2011/05/12
Key code:
  308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18BD
  96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC1E
  DBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE01941D
  DD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36895038
  7811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
  4EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD
  35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC717B6123
  91C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1
  585DA7F42519718CC9B09EEF0381850002818100A1E456C8DA2AD1BB83B1BDF2A1A6B5A6E8
  3642B460402445DA7E4036715F468F76655E114D460B7112F57143EE020AEF4A5BFAD07B74
  0FBCB1C64DA8A2BCE619283421445EEC77D3CF0D11866E9656AD6511F4926F8376967B0AB7
  15F9FB7B514BC1174155DD6E073B1FCB3A2749E6C5FEA81003E16729497D0EAD9105E3E76A
```

ローカル ECDSA 鍵ペア **ecdsa1** の公開鍵を表示します。

<AP> display public-key local ecdsa public name ecdsa1

```
==========================================
Key name: ecdsa1
Key type: ECDSA
Key length: 192
Time when key pair created: 15:43:33 2011/05/12
Key code:
3049301306072A8648CE3D020106082A8648CE3D03010103320004A1FB84D92315B8DB72D1
AE672C7CFA5135D5F5B02377F2F092F182EC83B5819795BC94CCBD3EBA7D4F0F2B2EB20C58
4D
```

表 4-1 コマンド出力

フィールド	説明
Key name	ローカル鍵ペアの名前です。 鍵ペアを作成したとき、名前を指定しない場合、以下の鍵ペア名の後ろに（default）が追加されます。 以下に各鍵アルゴリズムのデフォルト鍵ペアを示します。 • **hostkey**—デフォルトRSAホスト鍵ペア名です。 • **serverkey**—デフォルトRSAサーバ鍵ペア名です。 • **dsakey**—デフォルトDSAホスト鍵ペア名です。
Key type	オプションです。 • **RSA** • **DSA**
Time when key pair created	ローカル鍵ペアが作成された日時です。
Key code	公開鍵の文字列です。

関連コマンド

public-key local create

4.1.2 display public-key peer

Syntax

display public-key peer [**brief** | **name** *publickey-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

brief: すべてのピアのホスト公開鍵の概要を表示します。鍵タイプ、鍵モジュール、鍵名のみ表示します。

name *publickey-name*: ピアのホスト公開鍵の詳細情報を表示します。鍵コードが含まれます。*publickey-name* はピアのホスト公開鍵の名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

display public-key peer コマンドはピアのホスト公開鍵の情報を表示します。

パラメータを指定しない場合、ローカル装置で設定したすべてのピアのホスト公開鍵の詳細情報を表示します。

ローカル装置のピアのホスト公開鍵を設定する場合、**public-key peer** コマンドあるいは **public-key peer import sshkey** コマンドを使用します。

例

ピアのホスト公開鍵 idrsa の詳細情報を表示します。

<AP> display public-key peer name idrsa

```
=========================================
Key name: idrsa
Key type: RSA
Key modulus: 1024
Key code:
  30819F300D06092A864886F70D010101050003818D0030818902818100C5971581A78B5388
  B3C9063EC6B53D395A6704D9752B6F9B7B1F734EEB5DD509F0B050662C46FFB8D27F797E37
  918F6270C5793F1FC63638970A0E4D51A3CEF7CFF6E92BFAFD73F530E0BDE27056E81F2525
  6D0883836FD8E68031B2C272FE2EA75C87734A7B8F85B8EBEB3BD51CC26916AF3B3FDC32C3
  42C142D41BB4884FEB0203010001
```

表 4-2 コマンド出力

フィールド	説明
Key name	ピアのホスト公開鍵の名前です。
Key type	鍵タイプです。RSA、DSAがあります。
Key modulus	鍵モジュール長です。単位はビットです。
Key code	公開鍵の文字列です。

すべてのピアのホスト公開鍵の概要情報を表示します。

<AP> display public-key peer brief

```
Type  Modulus  Name
---------------------------
RSA   1024    idrsa
```

```
DSA   1024    10.1.1.1
```

表 4-3 コマンド出力

フィールド	説明
Type	鍵タイプです。RSA、DSAがあります。
Modulus	鍵モジュール長です。単位はビットです。
Name	ピアの公開鍵の名前です。

関連コマンド

- **public-key peer**
- **public-key peer import sshkey**

4.1.3 peer-public-key end

Syntax

peer-public-key end

View

Public key view

定義済みユーザロール

network-admin

説明

peer-public-key end コマンドは public key view から system view に戻り、設定されたピアのホスト公開鍵を保存します。

ローカル装置でピアのホスト公開鍵を入力した後、このコマンドを使用し、public key view から system view に戻り、ホスト公開鍵を保存します。

システムは公開鍵を保存する前に確認します。鍵が正しい形式でない場合、システムは鍵を廃棄し、エラーメッセージを表示します。鍵が正常である場合、鍵を保存します。鍵はたとえば、**display public-key local public** コマンドで表示することができます。

例

public key view から system view に戻り、設定されたピアのホスト公開鍵を保存します。

<AP> system-view

[AP] public-key peer key1

```
Enter public key view. Return to system view with "peer-public-key end" command.
```

[AP-pkey-public-key-key1]30819F300D06092A864886F70D010101050003818D003081
8902818100C0EC8014F82515F6335A0A

[AP-pkey-public-key-key1]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308C
29481B77E719D1643135877E13B1C531B4

[AP-pkey-public-key-key1]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B854
E2371D5B952ADF6B80EB5F52698FCF3D6

[AP-pkey-public-key-key1]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276
FFD4AF2050BD4A9B1DDE675AC30CB020301

[AP-pkey-public-key-key1]0001

[AP-pkey-public-key-key1] peer-public-key end

[AP]

関連コマンド

- **display public-key local public**
- **display public-key peer**
- **public-key peer**

4.1.4 public-key local create

Syntax

public-key local create { **dsa** | **ecdsa** [**secp192r1** | **secp256r1** | **secp384r1**
| **secp521r1**] | **rsa** } [**name** key-name]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

dsa: DSA 鍵ペアを作成します。

ecdsa: ECDSA 鍵ペアを作成します。

- **secp192r1**: secp192r1 使用して、192 ビットの ECDSA 鍵ペアを作成します。
- **secp256r1**: secp256r1 使用して、256 ビットの ECDSA 鍵ペアを作成します。
- **secp384r1**: secp384r1 使用して、384 ビットの ECDSA 鍵ペアを作成します。
- **secp521r1**: secp521r1 使用して、521 ビットの ECDSA 鍵ペアを作成します。

デフォルトでは、secp192r1 が使用されます。

rsa: RSA 鍵ペアを作成します。

name *key-name*: ローカル非対称鍵ペアの名前を割り当てます。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を割り当てない場合、デフォルト名を適用します。

表 4-4 デフォルトのローカル鍵ペア名

タイプ	デフォルト名
RSA	• **ホスト鍵ペア**：hostkey • **サーバ鍵ペア**：serverkey
DSA	dsakey
ECDSA	ecdsakey

説明

public-key local create コマンドはローカル非対称鍵ペアを作成します。

鍵アルゴリズムはセキュリティアプリケーションで要求されたアルゴリズムと同一にする必要があります。

鍵の長さは適切に設定する必要があります。鍵の長さが長いと高いセキュリティとなりますが、鍵を作成する時間も長くなります。

鍵の長さは表 5-5 に示すように非対称鍵アルゴリズムの異なるタイプの比較を示します。

鍵ペアの名前を割り当てない場合、デフォルトの名前を割り当て、鍵ペアを default としてマーキングします。デフォルトの名前を別の鍵ペアに割り当てることができますが、鍵ペアを default としてマーキングしません。鍵ペアの名前は、同じ鍵アルゴリズムを使用する鍵ペア間で一意にする必要がありますが、異なる鍵アルゴリズムを使用する鍵ペアでは同じ名前を使用することができます。もし名前が重複している場合、存在する鍵ペアに上書きしていいか確認メッセージが表示されます。

鍵ペアは自動で保存され、装置の再起動が行われても削除されません。

表 4-5 非対称鍵アルゴリズムの異なるタイプの比較

タイプ	鍵ペア数	モジュール長	推奨
RSA	• 鍵ペアの名前を指定する場合、ホスト鍵ペアを作成します。 • 鍵ペアの名前を指定しない場合、1つのサーバ鍵ペアと1つのホスト鍵ペアを作成し、デフォルト名を使用します。	設定範囲は512～2048ビットです。 デフォルトは1024ビットです。	少なくとも768ビットにしてください。
DSA	1つのホスト鍵ペアを作成します。	設定範囲は512～2048ビットです。 デフォルトは1024ビットです。	少なくとも768ビットにしてください。
ECDSA	1つのホスト鍵ペアを作成します。	設定できる長さ 192, 256, 384, or 521 bits.	ー

例

デフォルト名のローカル RSA 鍵ペアを作成します。

<AP> system-view

[AP] public-key local create rsa

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
```

```
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
.++++++
..++++++++
....++++++++
Create the key pair successfully.
```

デフォルト名のローカル DSA 鍵ペアを作成します。

<AP> system-view

[AP] public-key local create dsa

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.............
.......+.........+............+.........+...+.....+............+..+...
...+.................+.........+...+.+.......+.....+...........+.........+.
.........................+........+.......+.............+.....+...+.........
..............+.........+.........+........+........+....+.................
.....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

デフォルト名のローカル ECDSA 鍵ペアを作成します。

<AP> system-view

[AP] public-key local create ecdsa

```
Generating Keys...
Create the key pair successfully.
```

名前が rsa1 のローカル RSA 鍵ペアを作成します。

<AP> system-view

[AP] public-key local create rsa name rsa1

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...++++++
.............................++++++
Create the key pair successfully.
```

名前が dsa1 のローカル DSA 鍵ペアを作成します。

<AP> system-view

[AP] public-key local create dsa name dsa1

```
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.++++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+.................
.......+..........+.............+..........+...+.....+...............+..+...
...+..................+..........+...+.+.......+.....+............+.........+.
.........................+........+.......+..............+.....+...+..........
..............+.........+..........+........+........+....+..................
.....++++++++++++++++++++++++++++++++++++++++++++++++++*
Create the key pair successfully.
```

名前が **ecdsa1** のローカル ECDSA 鍵ペアを作成します。

<AP> system-view

[AP] public-key local create ecdsa name ecdsa1

```
Generating Keys...
Create the key pair successfully.
```

関連コマンド

- **display public-key local public**
- **public-key local destroy**

4.1.5 public-key local destroy

Syntax

public-key local destroy { **dsa** | **ecdsa** | **rsa** } [**name** *key-name*]

View

System view

定義済みユーザロール

network-admin

パラメータ

dsa: DSA タイプを指定します。

ecdsa: ECDSA タイプを指定します。

rsa: RSA タイプを指定します。

name *key-name*: ローカル非対称鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を指定しない場合、デフォルト名のローカル鍵ペアの指定されたタイプを削除します。

説明

public-key local destroy コマンドはローカル鍵ペアを削除します。

以下の状況が発生した場合、鍵を正常に保つため、ローカル非対称鍵ペアを削除し、新しいペアを生成する必要があります。

- 不正侵入が発生した場合。
- 装置の記憶媒体を交換した場合。
- ローカル証明書が期限切れとなった場合。ローカル証明書の詳細はオペレーションマニュアルのセクション 13 *“セキュリティ”* を参照してください。

例

デフォルト名のローカル RSA 鍵ペアを削除します。

<AP> system-view

[AP] public-key local destroy rsa

```
Confirm to destroy the key pair? [Y/N]:y
```

デフォルト名のローカル DSA 鍵ペアを削除します。

<AP> system-view

[AP] public-key local destroy dsa

```
Confirm to destroy the key pair? [Y/N] :y
```

デフォルト名のローカル ECDSA 鍵ペアを削除します。

<AP> system-view

[AP] public-key local destroy ecdsa

```
Confirm to destroy the key pair? [Y/N]:y
```

名前が rsa1 のローカル RSA 鍵ペアを削除します。

<AP> system-view

[AP] public-key local destroy rsa name rsa1

```
Confirm to destroy the key pair? [Y/N]:y
```

名前が dsa1 のローカル DSA 鍵ペアを削除します。

<AP> system-view

[AP] public-key local destroy dsa name dsa1

```
Confirm to destroy the key pair? [Y/N] :y
```

名前が **ecdsa1** のローカル ECDSA 鍵ペアを削除します。

<AP> system-view

[AP] public-key local destroy ecdsa name ecdsa1

```
Confirm to destroy the key pair? [Y/N] :y
```

関連コマンド

public-key local create

4.1.6 public-key local export dsa

Syntax

public-key local export dsa [**name** *key-name*] { **openssh** | **ssh2** } [*filename*]

View

System view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: ローカル DSA 鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。指定しない場合、デフォルト名のローカル DSA 鍵ペアのホスト公開鍵を表示あるいはエクスポートします。

openssh: OpenSSH の形式を使用します。

ssh2: SSH2.0 の形式を使用します。

filename: 保存するローカルホスト公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。”./”、”../” を除いて指定します。名前は、ドット（.）、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュ(/)にすることができません。ファイル名の詳細はオペレーションマニュアルのセクション 1 *基本機能 “ファイルシステム管理”* を参照してください。

説明

public-key local export dsa コマンドは指定した形式のローカル DSA ホスト公開鍵を表示あるいはファイルにエクスポートします。

filename が指定されている場合、ローカル DSA ホスト公開鍵をエクスポートします。指定されていない場合、ローカル DSA ホスト公開鍵を表示します。

ローカル DSA ホスト公開鍵をピアの装置に分配する前に、コマンドを使用して表示あるいはエクスポートすることができます。

1) ローカルホスト公開鍵を以下のいずれかの方法でファイルに保存します。
   - **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** }コマンドを使用し、指定した形式のローカルホスト公開鍵を表示します。内容をコピーし、ファイルにペーストします。
   - **public-key local export dsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* コマンドを使用し、ファイルにローカルホスト公開鍵をエクスポートします。ホスト公開鍵をフォルダ pkey あるいはサブフォルダにエクスポートすることはできません。
2) バイナリモードの FTP あるいは TFTP などを使用してファイルのコピーをピアの装置に転送します。FTP、TFTP の詳細はオペレーションマニュアルのセクション 1 *基本機能 “FTP と TFTP”* を参照してください。

3) ピアの装置でファイルから **public-key peer import sshkey** コマンドを使用してホスト公開鍵をインポートします。

SSH2.0 と OpenSSH は異なる公開鍵形式です。ホスト公開鍵をインポートする装置でサポートされる形式に従って適切に選択してください。

例

OpenSSH 形式のデフォルト名のローカル DSA 鍵ペアのホスト公開鍵をファイル key.pub にエクスポートします。

<AP> system-view

[AP] public-key local export dsa openssh key.pub

SSH2.0 形式のデフォルト名のローカル DSA 鍵ペアのホスト公開鍵を表示します。

<AP> system-view

[AP] public-key local export dsa ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBt
YcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3sTwmIflQeweU
wLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo=
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のデフォルト名のローカル DSA 鍵ペアのホスト公開鍵を表示します。

<AP> system-view

[AP] public-key local export dsa openssh

```
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACAQZEs400SvNIVfnqxwvA7PvOVEA89tKni/f6GDBvWY9Z2Q499pAqUBt
YcqQea8T4zBInxx2eF3lLaZJrIvAS205zXxSzQoU9190kakdMdasIjQLWYGyepFc3sTwmIflQeweU
wLVAPaOesKaCERjxg+e4maYWlAvySGT4c9NJlxLo= dsa-key
```

OpenSSH 形式のローカル DSA 鍵ペア dsa1 のホスト公開鍵をファイル dsa1.pub にエクスポートします。

<AP> system-view

[AP] public-key local export dsa name dsa1 openssh dsa1.pub

SSH2.0 形式のローカル DSA 鍵ペア dsa1 のホスト公開鍵を表示します。

<AP> system-view

[AP] public-key local export dsa name dsa1 ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-2011/05/12"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3
ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7CrcV+ft7UUv
BF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のローカル DSA 鍵ペア dsa1 のホスト公開鍵を表示します。

<AP> system-view

[AP] public-key local export dsa name dsa1 openssh

```
ssh-dss
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06UiL+CM7OZb5
sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd3Xf+axKJPadu68HRKN
l/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIE
AgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UI
LiLFs3ThbdABMs5xsCAhcJGscXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9
LFYXaf0JRlxjMmwnu8AAACBAKHkVsjaKtG7g7G98qGmtaboNkK0YEAkRdp+QDZxX0aPdmVeEU1GC3
ES9XFD7gIK70pb+tB7dA+8scZNqKK85hkoNCFEXux3088NEYZullatZRH0km+DdpZ7CrcV+ft7UUv
BF0FV3W4HOx/LOidJ5sX+qBAD4WcpSX0OrZEF4+dq dsa-key
```

関連コマンド

- **public-key local create**
- **public-key peer import sshkey**

4.1.7 public-key local export rsa

Syntax

public-key local export rsa [**name** *key-name*] { **openssh** | **ssh1** | **ssh2** } [*filename*]

View

System view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: ローカル RSA 鍵ペアの名前を指定します。設定範囲は 1～64 文字です。英字、数字、ハイフン（-）を含みます。名前を指定しない場合、デフォルト名のローカル鍵 RSA ペアのホスト公開鍵を表示あるいはエクスポートします。

openssh: OpenSSH の形式を使用します。

ssh1: SSH1.5 の形式を使用します。

ssh2: SSH2.0 の形式を使用します。

filename: 保存するローカルホスト公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。”./”、”../” を除いて指定します。名前は、ドット（.）、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュ(/)にすることができません。ファイル名の詳細はオペレーションマニュアルのセクション 1 *基本機能 “ファイルシステム管理”* を参照してください。

説明

public-key local export rsa コマンドは指定した形式のローカル RSA ホスト公開鍵を表示あるいはファイルにエクスポートします。

filename が指定されている場合、ローカル RSA ホスト公開鍵をエクスポートします。指定されていない場合、ローカル RSA ホスト公開鍵を表示します。

ローカル DSA ホスト公開鍵をピアの装置に分配する前に、コマンドを使用して表示あるいはエクスポートすることができます。

1) ローカルホスト公開鍵を以下のいずれかの方法でファイルに保存します。
   - **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } コマンドを使用し、指定した形式のローカルホスト公開鍵を表示します。内容をコピーし、ファイルにペーストします。
   - **public-key local export rsa** [**name** *key-name*] { **openssh** | **ssh2** } *filename* コマンドを使用し、ファイルにローカルホスト公開鍵をエクスポートします。ホスト公開鍵をフォルダ pkey あるいはサブフォルダにエクスポートすることはできません。
2) バイナリモードの FTP あるいは TFTP などを使用してファイルのコピーをピアの装置に転送します。FTP、TFTP の詳細はオペレーションマニュアルのセクション 1 *基本機能 “FTP と TFTP”* を参照してください。
3) ピアの装置でファイルから **public-key peer import sshkey** コマンドを使用してホスト公開鍵をインポートします。

SSH1.5、SSH2.0、OpenSSH は異なる公開鍵形式です。ホスト公開鍵をインポートする装置でサポートされる形式に従って適切に選択してください。

例

OpenSSH 形式のデフォルト名のローカル RSA 鍵ペアのホスト公開鍵をファイル key.pub にエクスポートします。

<AP> system-view

[AP] public-key local export rsa openssh key.pub

SSH2.0 形式のデフォルト名のローカル RSA 鍵ペアのホスト公開鍵を表示します。

<AP> system-view

[AP] public-key local export rsa ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGM
rSfddq/bYcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvy
vPJilneKJqhPT0xdv4tlas+mLNloY0dImbwS2kwE71rgg1CQ==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のデフォルト名のローカル RSA 鍵ペアのホスト公開鍵を表示します。

<AP> system-view

[AP] public-key local export rsa openssh

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDapKr+/gTCyWZyabuCJuJjMeMPQaj/kixzOCCAl+hDMmEGM
rSfddq/bYcbgM7Buit1AgB3x0dFyTPi85DcCznTW4goPXAKFjuzCbGfj4chakSr+/aj1k3rM+XOvy
vPJilneKJqhPT0xdv4tlas+mLNloY0dImbwS2kwE71rgg1CQ== rsa-key
```

OpenSSH 形式のローカル RSA 鍵ペア rsa1 のホスト公開鍵をファイル rsa1.pub にエクスポートします。

<AP> system-view

[AP] public-key local export rsa name rsa1 openssh rsa1.pub

SSH2.0 形式のローカル RSA 鍵ペア rsa1 のホスト公開鍵を表示します。

<AP> system-view

[AP] public-key local export rsa name rsa1 ssh2

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-2011/05/12"
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J0
0fBQ8XY+q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05
t8mCLVaupbfCzP8ba8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ==
---- END SSH2 PUBLIC KEY ----
```

OpenSSH 形式のローカル RSA 鍵ペア rsa1 のホスト公開鍵を表示します。

<AP> system-view

[AP] public-key local export rsa name rsa1 openssh

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDevEbyF93xHUJucJWqRc1r8fhzQ9lSVprCI6ATZeDYyR1J0
0fBQ8XY+q2olqoagn5YDyUC8ZJvUhlyMOHeORpkAVxD3XncTp4XG66h3rTHHa7Xmm7f1GDYlF0n05
t8mCLVaupbfCzP8ba8UkrUmMO4fUvW6zavA5LYxtlAiQv0KQ== rsa-key
```

関連コマンド

- **public-key local create**
- **public-key peer import sshkey**

4.1.8 public-key peer

Syntax

public-key peer *keyname*

undo public-key peer *keyname*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyname: ピアの公開鍵の名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

説明

public-key peer コマンドはピアの公開鍵の名前を指定し、public key view に移行します。

undo public-key peer コマンドはピアの公開鍵を削除します。

public key view に移行するため、コマンドを実行した後、公開鍵を入力します。半角スペースと改行は入力できますが、保存されません。

ローカル装置でピアの公開鍵を手動で指定するため、最初に 16 進数のピアの公開鍵を取得し、ローカル装置で以下の処理を行ってください。

1) public key view に移行するため、**public-key peer** コマンドを実行します。
2) 公開鍵を入力します。
3) **peer-public-key end** コマンドを実行し、公開鍵を保存し、system view に戻ります。

public key view で正しい形式の公開鍵を入力してください。ピアの装置が QX シリーズである場合、公開鍵を記録するため、**display public-key local public** コマンドを使用することを推奨します。

例

ピアの公開鍵 key1 を指定し、public key view に移行します。

<AP> system-view

[AP] public-key peer key1

```
Enter public key view. Return to system view with "peer-public-key end" command.
```

[AP-pkey-public-key-key1]

関連コマンド

- **display public-key local public**
- **display public-key peer**
- **peer-public-key end**

4.1.9 public-key peer import sshkey

Syntax

public-key peer *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

keyname: ピアの公開鍵の名前を指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

filename: 保存するピアの公開鍵の名前を指定します。設定範囲は 1～128 文字です。大文字、小文字を区別しません。"./"、"../"を除いて指定します。名前は、ドット(.)、hostkey、serverkey、dsakey、ecdsakey を使用することができません。また先頭をスラッシュ(/)にすることができません。ファイル名の詳細はオペレーションマニュアルのセクション 1 *基本機能　"ファイルシステム管理"* を参照してください。

説明

public-key peer import sshkey コマンドは公開鍵ファイルからピアのホスト公開鍵をインポートします。

undo public-key peer コマンドは指定したピアのホスト公開鍵を削除します。

ピアのホスト公開鍵をインポートする前に、バイナリモードで FTP または TFTP を使用してピアの装置から公開鍵のファイルのコピーの取得を行ってください。

このコマンドを設定した後、システムは自動的に PKCS（Public Key Cryptography Standards）形式にホスト公開鍵を変換し、保存します。

装置は SSH1.5、SSH2.0、OpenSSH の形式の公開鍵をインポートすることができます。

例

公開鍵ファイル key.pub からピアのホスト公開鍵 key2 をインポートします。

<AP> system-view

[AP] public-key peer key2 import sshkey key.pub

関連コマンド

- **display public-key peer**
- **public-key local export dsa**
- **public-key local export rsa**

目次

このセクションのページは **13-x-x** です。

5 章 SSH 5-1
5.1 SSH サーバ設定コマンド 5-1
5.1.1 display ssh server 5-1
5.1.2 display ssh user-information 5-4
5.1.3 sftp server enable 5-5
5.1.4 sftp server idle-timeout 5-7
5.1.5 ssh server acl 5-8
5.1.6 ssh server authentication-retries 5-9
5.1.7 ssh server authentication-timeout 5-11
5.1.8 ssh server compatible-ssh1x enable 5-12
5.1.9 ssh server dscp 5-13
5.1.10 ssh server enable 5-14
5.1.11 ssh server rekey-interval 5-16
5.1.12 ssh user 5-17
5.2 SSH クライアント設定コマンド 5-20
5.2.1 bye 5-20
5.2.2 cd 5-21
5.2.3 cdup 5-22
5.2.4 delete 5-23
5.2.5 dir 5-24
5.2.6 display sftp client source 5-26
5.2.7 display ssh client source 5-27
5.2.8 exit 5-28
5.2.9 get 5-29
5.2.10 help 5-30
5.2.11 ls 5-32
5.2.12 mkdir 5-34
5.2.13 put 5-35
5.2.14 pwd 5-36
5.2.15 quit 5-37
5.2.16 remove 5-38
5.2.17 rename 5-39
5.2.18 rmdir 5-40
5.2.19 scp 5-41
5.2.20 sftp 5-45
5.2.21 sftp client source 5-48

5.2.22 ssh client source..... 5-49
5.2.23 ssh2..... 5-50

5章 SSH

5.1 SSHサーバ設定コマンド

5.1.1 display ssh server

Syntax

display ssh server { **session** | **status** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

session: SSH サーバのセッションを表示します。

status: SSH サーバの状態を表示します。

説明

display ssh server コマンドは SSH サーバで SSH サーバのセッションあるいは状態を表示します。

例

SSH サーバの状態を表示します。

<AP> display ssh server status

```
Stelnet server: Disable
SSH version : 2.0
SSH authentication-timeout : 60 second(s)
SSH server key generating interval : 0 hour(s)
SSH authentication retries : 3 time(s)
SFTP server: Disable
SFTP server Idle-Timeout: 10 minute(s)
NETCONF server: Disable
SCP server: Disable
SSH Server PKI domain name: aaa
```

表 5-1 コマンド出力

フィールド	説明
Stelnet server	Stelnetサーバ機能が有効かどうかを示します。
SSH version	SSHプロトコルのバージョンです。 SSH1をサポートしている場合、プロトコルバージョンは1.99です。その他の場合、プロトコルバージョンは2です。
SSH authentication-timeout	認証タイムアウトタイマです。
SSH server key generating interval	SSHサーバ鍵ペアのアップデート間隔です。
SSH authentication retries	SSHユーザの認証の最大試行回数です。
SFTP server	SFTPサーバ機能が有効かどうかを示します。
SFTP server Idle-Timeout	SFTP接続アイドルタイムアウトタイマです。
Netconf server	NETCONF over SSHが有効かどうかを示します。
SCP server	SCPサーバ機能が有効かどうかを示します。
SSH Server PKI domain name	SSHサーバで指定したPKIドメインの名前です。

SSH サーバのセッションを表示します。

<AP> display ssh server session

```
UserPid   SessID Ver   Encrypt    State        Retries  Serv     Username
 184      0     2.0   aes128-cbc Established    1       Stelnet  abc@123
```

表 5-2 コマンド出力

フィールド	説明
UserPid	ユーザプロセスIDです。
SessID	セッションIDです。
Ver	SSHサーバのプロトコルバージョンです。
Encrypt	SSHサーバで使用される暗号化アルゴリズムです。
State	セッション状態です。 • **Init**–初期化状態です。 • **Ver-exchange**–バージョンのネゴシエーション状態です。 • **Keys-exchange**–鍵交換状態です。

フィールド	説明
	• **Auth-request**–認証要求状態です。 • **Serv-request**–セッションサービス要求状態です。 • **Established**–セッションが確立されています。 • **Disconnected**–セッションが切断されています。
Retries	認証に失敗した数です。
Serv	サービスタイプです。 • SCPです。 • SFTPです。 • Stelnetです。 • NETCONFです。
Username	サーバにログインしているユーザ名です。

5.1.2 display ssh user-information

Syntax

display ssh user-information [*username*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

username: SSH ユーザ名を指定します。設定範囲は 1～80 文字です。大文字、小文字を区別します。指定しない場合、すべての SSH ユーザの情報を表示します。

説明

display ssh user-information コマンドは SSH サーバの SSH ユーザの情報を表示します。

このコマンドは、SSH サーバ上で **ssh user** コマンドを使用して設定された SSH ユーザのみの情報を表示します。

例

すべての SSH ユーザの情報を表示します。

<AP> display ssh user-information

```
Total ssh users:2
Username          Authentication-type  User-public-key-name  Service-type
yemx              password                                   Stelnet|SFTP
test              publickey          pubkey                  SFTP
```

表 5-3 コマンド出力

フィールド	説明
Total ssh users	SSHユーザの総数です。
Authentication-type	認証方式です。 ● パスワード認証です。 ● 公開鍵認証です。 ● パスワード-公開鍵認証です。 ● 他の認証です。

フィールド	説明
User-public-key-name	ユーザの公開鍵名です。パスワード認証が使用される場合、表示されません。
Service-type	サービスタイプです。 ● Stelnetです。 ● SFTPです。 ● SCPです。 ● NETCONFです。 SSHユーザで複数のサービスタイプが有効である場合、垂直バー（|）で区切られます。

関連コマンド

ssh user

5.1.3 sftp server enable

Syntax

sftp server enable

undo sftp server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

sftp server enable コマンドは SFTP サーバ機能を有効にします。

undo sftp server enable コマンドは SFTP サーバ機能を無効にします。

例

SFTP サーバ機能を有効にします。

<AP> system-view

[AP] sftp server enable

関連コマンド

display ssh server

5.1.4 sftp server idle-timeout

Syntax

sftp server idle-timeout *time-out-value*

undo sftp server idle-timeout

デフォルト

10 分

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value: タイムアウトタイマを指定します。設定範囲は 1～35791 分です。

説明

sftp server idle-timeout コマンドは SFTP サーバの SFTP ユーザ接続のアイドルタイムアウトタイマを設定します。

undo sftp server idle-timeout コマンドはデフォルトに戻します。

アイドルタイムアウトタイマが終了したとき、SFTP 接続がアイドルである場合、システムは自動的に接続を切断します。多くの SFTP 接続が確立されている場合、接続リソースを即座に開放できるように、タイマを小さい値に設定することができます。

例

SFTP ユーザ接続のアイドルタイムアウトタイマを 500 分に設定します。

<AP> system-view

[AP] sftp server idle-timeout 500

関連コマンド

display ssh server

5.1.5 ssh server acl

Syntax

ssh server acl { *advanced-acl-number* | *basic-acl-number* | **mac** *mac-acl-number* }

undo ssh server acl

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

advanced-acl-number: 拡張 IPv4 ACL を指定します。設定範囲は 3000～3999 です。

basic-acl-number: 標準 IPv4 ACL を指定します。設定範囲は 2000～2999 です。

mac *mac-acl-number:* L2 ACL を指定します。設定範囲は 4000～4999 です。

説明

ssh server acl コマンドは IPv4 SSH サーバへのアクセスを制御します。

undo ssh server acl コマンドはデフォルトに戻します。

ACL を使用して IPv4 SSH クライアントの要求パケットをフィルタするために使用します。

- ACL ルールが設定されている場合、ACL の permit 条件に一致する IPv4 SSH クライアントの要求パケットのみがサーバにアクセスすることができます。
- ACL ルールが存在しない、あるいは ACL に条件がない場合、すべての IPv4 SSH クライアントがサーバにアクセスすることができます。

この設定は、設定した後に SSH 接続を行った要求パケットから有効になります。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

IPv4 SSH クライアント 1.1.1.1 のみサーバにアクセスできるように ACL 2001 を設定します。

<AP> system-view

[AP] acl basic 2001

[AP-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0

[AP-acl-ipv4-basic-2001] quit

[AP] ssh server acl 2001

関連コマンド

display ssh server

5.1.6 ssh server authentication-retries

Syntax

ssh server authentication-retries *retries*

undo ssh server authentication-retries

デフォルト

3

View

System view

定義済みユーザロール

network-admin

パラメータ

retries: SSH ユーザの認証を試行する最大数を指定します。設定範囲は 1～5 です。

説明

ssh server authentication-retries コマンドは SSH ユーザの認証を試行する最大数を指定します。

undo ssh server authentication-retries コマンドはデフォルトに戻します。

偽のユーザ名とパスワードの攻撃を防ぐため、最大数を設定することができます。

- 認証が使用されたとき、公開鍵とパスワード認証の合計の試行回数が設定した上限を超えることができません。
- 認証方式がパスワード-公開鍵である場合、SSH ユーザを認証するため、最初にサーバは公開鍵認証を使用し、ユーザパスワード認証を使用します。プロセスは 1 つの認証を行うものとして扱います。

この設定はログインユーザには適用されません。新しい SSH ユーザのみ適用されます。

例

SSH ユーザの認証を試行する最大数を 4 に設定します。

<AP> system-view

[AP] ssh server authentication-retries 4

関連コマンド

display ssh server

5.1.7 ssh server authentication-timeout

Syntax

ssh server authentication-timeout *time-out-value*

undo ssh server authentication-timeout

デフォルト

60 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

time-out-value: 認証タイムアウトタイマを指定します。設定範囲は 1～120 秒です。

説明

ssh server authentication-timeout コマンドは SSH サーバで SSH ユーザ認証のタイムアウトタイマを設定します。

undo ssh server authentication-timeout コマンドはデフォルトに戻します。

タイムアウトタイマが終了したとき、ユーザが認証を終了しない場合、接続は確立することができません。

タイムアウトタイマの値を小さくすることで、認証が中断される間に、偽の TCP 接続による占有を防ぐことができます。

例

SSH ユーザ認証のタイムアウトタイマを 10 秒に設定します。

<AP> system-view

[AP] ssh server authentication-timeout 10

関連コマンド

display ssh server

5.1.8 ssh server compatible-ssh1x enable

Syntax

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x [enable]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

network-operator

説明

ssh server compatible-ssh1x enable コマンドは SSH1 クライアントをサポートする SSH サーバを有効にします。

undo ssh server compatible-ssh1x コマンドは SSH サーバで SSH1 クライアントのサポートを無効にします。

この設定はログインユーザには適用されません。次回ログインしたユーザのみ適用します。

例

SSH1 クライアントをサポートする SSH サーバを有効にします。

<AP> system-view

[AP] ssh server compatible-ssh1x enable

関連コマンド

display ssh server

5.1.9 ssh server dscp

Syntax

ssh server dscp *dscp-value*

undo ssh server dscp

デフォルト

48

View

System view

定義済みユーザロール

network-admin

パラメータ

dscp-value: 送信 IPv4 パケットの DHCP を指定します。設定範囲は 0〜63 です。DSCP の値が大きくなると、プライオリティが高くなります。

説明

ssh server dscp コマンドは SSH サーバが SSH クライアントに IPv4 パケットを送信する DHCP を設定します。

undo ssh server dscp コマンドはデフォルトに戻します。

DHCP パケットの DSCP の値はパケットのプライオリティを指定します。パケットを送信するプライオリティに影響します。

例

SSH サーバによって送信される IPv4 パケットの DSCP を 30 に設定します。

<AP> system-view

[AP] ssh server dscp 30

5.1.10 ssh server enable

Syntax

ssh server enable

undo ssh server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

ssh server enable コマンドは Stelnet サーバ機能を有効にします。

undo ssh server enable コマンドは Stelnet サーバ機能を無効にします。

例

Stelnet サーバ機能を有効にします。

<AP> system-view

[AP] ssh server enable

関連コマンド

display ssh server

5.1.11 ssh server port

Syntax

ssh server port *port-number*

undo ssh server port

デフォルト

SSH server port：22

View

System view

定義済みユーザロール

network-admin

パラメータ

port-number: ポート番号を 1～65535 の範囲で指定します。

説明

ssh server port を使用して SSH サービスポートを指定します。

undo ssh server port を使用してデフォルトに戻します。

⚠ **注意:**

- SSH サーバが有効な状態で SSH ポート番号を変更すると、変更後は、SSH サービスが再起動し、すべての SSH 接続が切断されます。SSH ユーザがサーバにアクセスする場合は、SSH サーバに再接続してください。
- SSH ポートを well-known ポート番号に設定した場合、well-known ポート番号を使用したサービスが起動できない場合があります。well-known ポート番号として設定できる範囲は 1～1024 です。

例

SSH サービスポートを 1025 に設定します。

<AP> system-view

[AP] ssh server port 1025

5.1.12 ssh server rekey-interval

Syntax

ssh server rekey-interval *interval*

undo ssh server rekey-interval

デフォルト

アップデート間隔の値は 0 時間です。RSA サーバ鍵ペアのアップデートを行いません。

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: RSA サーバ鍵ペアのアップデート間隔を指定します。設定範囲は 1～24 時間です。

説明

ssh server rekey-interval コマンドは RSA サーバ鍵ペアのアップデート間隔を設定します。

undo ssh server rekey-interval コマンドはデフォルトに戻します。

RSA サーバ鍵ペアを定期的にアップデートすることで、鍵ペアのハッキングを防ぎ、SSH 接続のセキュリティを強化することができます。

システムは SSH1 ユーザがサーバにログイン後にアップデート最小間隔を数え始めます。新しい SSH1 ユーザがアップデート最小間隔後にサーバにログインする場合、システムは以下の操作をします。

1) RSA サーバ鍵ペアをアップデートします。
2) 新しいユーザの鍵ペアネゴシエーションにアップデートされた RSA サーバ鍵ペアを使用します。
3) アップデート最小間隔を再び数え始めます。

例

RSA サーバ鍵ペアのアップデート間隔を 3 時間に設定します。

<AP> system-view

[AP] ssh server rekey-interval 3

関連コマンド

display ssh server

5.1.13 ssh user

Syntax

ssh user *username* **service-type** { **all** | **netconf** | **scp** | **sftp** | **stelnet** }

authentication-type { **password** | { **any** | **password-publickey** | **publickey** }

[**assign { pki-domain** domain-name **| publickey** *keyname* }] }

undo ssh user *username*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

username: SSH ユーザ名を指定します。設定範囲は 1〜80 文字です。大文字、小文字を区別します。ユーザ名に ISP ドメイン名が含まれる場合、*pureusername@domain* の形式になります。

service-type: SSH ユーザのサービスタイプを指定します。

- **all**: Stelnet、SFTP を指定します。
- **sftp**: SFTP のサービスタイプを指定します。
- **stelnet**: Stelnet のサービスタイプを指定します。

authentication-type: SSH ユーザの認証方法を指定します。

- **password**: パスワード認証を指定します。認証方式は容易で暗号時間が早くなりますが、セキュリティ強度は脆弱です。ユーザ認証、許可、アカウンティングを実行する AAA と同時に使用することができます。
- **any**: パスワード認証あるいは公開鍵認証のどちらかを指定します。
- **password-publickey**: SSH2 クライアントのパスワード認証と公開鍵認証の両方を指定します。SSH2 クライアントでは、**password-publickey** 認証方式は高いセキュリティを提供します。SSH1 クライアントではパスワード認証あるいは公開鍵認証のどちらかを指定します。
- **publickey**: 公開鍵認証を指定します。認証方式は複雑で暗号時間が遅いですが、セキュリティ強度は強くなり、総当たり攻撃（ブルートフォース攻撃）に対して防御することができます。この認証方式は、使用しやすいです。一度設定すると、パスワードを記憶しておくことやパスワードを入力することなく、認証プロセスが自動で完了します。

assign: クライアントを確認するために使用するパラメータを指定します。

- **pki-domain** domain-name: クライアントのデジタル証明書を検証する PKI ドメインを指定します。domain-name 引数は、大文字と小文字を区別しない 1 ～ 31 文字の文字列です。無効な文字は、チルダ (~)、アスタリスク (*)、バックスラッシュ (¥)、縦棒 (|)、コロン (:)、ドット (.)、山かっこ (< >)、引用符 (")、およびアポストロフィ (')。サーバは、PKI ドメインに保存されている CA 証明書を使用して、クライアントのデジタル証明書を検証します。このシナリオでは、サーバはクライアントの公開鍵を事前に保存する必要はありません。
- **publickey** *keyname*: SSH クライアントの公開鍵を指定します。*keyname* はサーバで設定される SSH クライアントの公開鍵を示します。設定範囲は 1～64 文字です。大文字、小文字を区別します。サーバはクライアントの確認を行うため、クライアントの公開鍵を使用します。もしクライアントの公開鍵のファイルが変更されている場合、すぐにサーバのクライアントの公開鍵をアップデートする必要があります。

説明

ssh user コマンドは SSH ユーザを作成し、サービスタイプと認証方式を指定します。

undo ssh user コマンドは SSH ユーザを削除します。

SSH ユーザを設定するため、認証方式に従ってコマンドを使用します。

- 認証方式が公開鍵である場合、SSH ユーザとローカルユーザを作成する必要があります。SSH ユーザが正しい作業ディレクトリとユーザロールを割り当てられるように、ローカルユーザは SSH ユーザのユーザ名と同一にする必要があります。
- 認証方式がパスワードである場合、SSH ユーザは以下の処理のどちらか 1 つを実行する必要があります。
  - ローカル認証用に、**local-user** コマンドを使用してローカルユーザを設定します。
  - リモート認証用に、RADIUS サーバのようなリモート認証サーバの SSH ユーザを設定します。

ssh user コマンドを使用して SSH ユーザを作成する必要がありません。しかし、集中管理のため、すべての SSH ユーザ（パスワード認証のみの SSH ユーザを含みます）を表示する場合、このコマンドを使用することができます。SSH ユーザが作成された場合、正しいサービスタイプと認証方式であることを確認してください。

- 認証方式が **password-publickey** あるいは **any** である場合、SSH ユーザは以下の処理のどちらか 1 つを実行する必要があります。
  - ローカル認証用に、**local-user** コマンドを使用してローカルユーザを設定します。
  - リモート認証用に、RADIUS サーバのようなリモート認証サーバの SSH ユーザを設定します。

どちらの場合でも、ローカルユーザあるいはリモート認証サーバで設定される SSH ユーザは SSH ユーザと同じユーザ名を使用する必要があります。

ホスト公開鍵を指定するため、このコマンドを複数回使用した場合、最後に行った設定が適用されます。ホスト公開鍵を指定しない場合、ユーザはログインを行うために証明書認証を使用します。

ユーザが SSH サーバと通信しているとき、SSH ユーザの認証方式、サービスタイプ、ホスト公開鍵を変更することができますが、設定の変更は次回ログインのクライアントのみ適用されます。

SFTP ユーザでは、作業ディレクトリは認証方式に依存します。

- 認証方式が **publickey** あるいは **password-publickey** である場合、作業ディレクトリは、関連した local user view で **authorization-attribute** コマンドを使用して指定されます。
- 認証方式がパスワードである場合､作業ディレクトリはAAAによって許可されます。

SSH ユーザでは、ユーザロールは認証方式に依存します。

- 認証方式が **publickey** あるいは **password-publickey** である場合、ユーザロールは関連した local user view で **authorization-attribute** コマンドを使用して指定されます。
- 認証方式がパスワードである場合､ユーザロールはリモート AAA サーバあるいはローカル装置によって許可されます。

例

SSH ユーザ user1 を作成します。ユーザにサービスタイプ sftp、認証方式 password-publickey を指定します。ユーザにホスト公開鍵 key1 を割り当てます。

<AP> system-view

[AP] ssh user user1 service-type sftp authentication-type password-publickey assign publickey key1

ローカル装置管理ユーザ user1 を作成します。プレーンテキストでパスワード 123456TESTplat&!を指定し、ユーザのサービスタイプ ssh を指定します。作業ディレクトリ flash:を割り当て、ユーザにユーザロール network-admin を割り当てます。

[AP] local-user user1 class manage

[AP-luser-manage-user1] password simple 123456TESTplat&!

[AP-luser-manage-user1] service-type ssh

[AP-luser-manage-user1] authorization-attribute work-directory flash: user-role network-admin

関連コマンド

- **authorization-attribute**
- **display ssh user-information**
- **local-user**
- **pki domain**

5.2 SSHクライアント設定コマンド

5.2.1 bye

Syntax

bye

View

SFTP client view

定義済みユーザロール

network-admin

説明

bye コマンドは SFTP サーバとの通信を終了し、user view に戻ります。

このコマンドは **exit** コマンド、**quit** コマンドと同一です。

例

SFTP サーバとの通信を終了し、user view に戻ります。

sftp> bye

<AP>

5.2.2 cd

Syntax

cd [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path: サーバのパスの名前を指定します。

説明

cd コマンドは SFTP サーバの作業パスを変更します。

上位のディレクトリに戻るため、**cd ..**コマンドを使用できます。

ルートディレクトリに戻るため、**cd /**コマンドを使用できます。

例

作業パスを new1 に変更します。

sftp> cd new1

```
Current Directory is:/new1
```

sftp> pwd

```
Remote working directory: /new1
```

sftp>

5.2.3 cdup

Syntax

cdup

View

SFTP client view

定義済みユーザロール

network-admin

説明

cdup コマンドは上位のディレクトリに戻ります。

例

現在の作業ディレクトリ/test1 から上位のディレクトリに戻ります。

sftp> cd test1

```
Current Directory is:/test1
```

sftp> pwd

```
Remote working directory: /test1
```

sftp> cdup

```
Current Directory is:/
```

sftp> pwd

```
Remote working directory: /
```

sftp>

5.2.4 delete

Syntax

delete *remote-file*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file: サーバから削除するファイルを指定します。

説明

delete コマンドはサーバからファイルを削除します。

このコマンドは **remove** コマンドと同一です。

例

サーバからファイル temp.c を削除します。

sftp> delete temp.c

```
Removing /temp.c
```

5.2.5 dir

Syntax

dir [**-a** | **-l**] [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

-a: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

-l: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリは除きます。

remote-path: ディレクトリの名前を指定します。指定しない場合、現在の作業ディレクトリの下にあるファイルとディレクトリの詳細情報を表示します。

説明

dir コマンドはディレクトリの下にあるファイルとサブディレクトリの情報を表示します。

-a あるいは**-l** のいずれも指定しない場合、ディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

このコマンドは **ls** コマンドと同一です。

例

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

sftp> dir -a

```
drwxrwxrwx    2 1       1             512 Dec 18 14:12 .
drwxrwxrwx    2 1       1             512 Dec 18 14:12 ..
-rwxrwxrwx    1 1       1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 012.pub
```

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

sftp> dir -l

```
-rwxrwxrwx    1 1       1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1       1             301 Dec 18 14:12 011.pub
```

```
-rwxrwxrwx    1 1       1            301 Dec 18 14:12 012.pu
```

🕮 **メモ：**

出力形式は、SSH サーバ装置モデルによって異なります。

5.2.6 display sftp client source

Syntax

display sftp client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display sftp client source コマンドは SFTP クライアントの送信元 IP アドレスを表示します。

例

SFTP クライアントの送信元 IP アドレスを表示します。

<AP> display sftp client source

```
The source IP address of the SFTP client is 192.168.0.1
```

関連コマンド

sftp client source

5.2.7 display ssh client source

Syntax

display ssh client source

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display ssh client source コマンドは Stelnet クライアントの送信元 IP アドレスを表示します。

例

Stelnet クライアントの送信元 IP アドレスを表示します。

<AP> display ssh client source

```
The source IP address of the SSH client is 192.168.0.1
```

関連コマンド

ssh client source

5.2.8 exit

Syntax

exit

View

SFTP client view

定義済みユーザロール

network-admin

network-operator

説明

exit コマンドは SFTP サーバとの通信を終了し、user view に戻ります。

このコマンドは **bye** コマンド、**quit** コマンドと同一です。

例

SFTP サーバとの通信を終了し、user view に戻ります。

sftp> exit

<AP>

5.2.9 get

Syntax

get *remote-file* [*local-file*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file: SFTP サーバの名前を指定します。

local-file: ローカルファイルの名前を指定します。指定しない場合、ファイルはサーバのファイルと同一の名前で保存されます。

説明

get コマンドは FTP サーバからファイルをダウンロードし、ローカルにファイルを保存します。

例

ファイル temp1.c をダウンロードし、ローカルにファイル temp.c として保存します。

sftp> get temp1.c temp.c

```
Fetching /temp1.c to temp.c
/temp.c                                       100% 1424     1.4KB/s   00:00
```

5.2.10 help

Syntax

help

View

SFTP client view

定義済みユーザロール

network-admin

説明

help コマンドは SFTP クライアントコマンドのヘルプ情報を表示します。

このコマンドはクォーテーションマーク（?）を入力した場合と同一です。

例

SFTP クライアントでヘルプ情報を表示します。

sftp> help

```
Available commands:
  bye                     Quit sftp
  cd [path]                Change remote directory to 'path'
  cdup                    Change remote directory to the parent directory
  delete path              Delete remote file
  dir [-a|-l][path]         Display remote directory listing
      -a                   List all filenames
      -l                   List filename including the specific
                           information of the file
  exit                    Quit sftp
  get remote-path [local-path] Download file
  help                    Display this help text
  ls [-a|-l][path]          Display remote directory
      -a                   List all filenames
      -l                   List filename including the specific
                           information of the file
  mkdir path               Create remote directory
  put local-path [remote-path] Upload file
  pwd                     Display remote working directory
  quit                    Quit sftp
  rename oldpath newpath     Rename remote file
  remove path              Delete remote file
  rmdir path               Delete remote empty directory
  ?                       Synonym for help
```

5.2.11 ls

Syntax

ls [**-a** | **-l**] [*remote-path*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

-a: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

-l: リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリは除きます。

remote-path: ディレクトリの名前を指定します。指定しない場合、現在の作業ディレクトリの下にあるファイルとディレクトリの詳細情報を表示します。

説明

ls コマンドはディレクトリの下にあるファイルとサブディレクトリの情報を表示します。

-a あるいは**-l** のいずれも指定しない場合、ディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

このコマンドは **dir** コマンドと同一です。

例

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。ドット（.）で始まる名前のファイルとサブディレクトリも含みます。

```
sftp> ls -a
drwxrwxrwx    2 1        1             512 Dec 18 14:12 .
drwxrwxrwx    2 1        1             512 Dec 18 14:12 ..
-rwxrwxrwx    1 1        1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1             301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1             301 Dec 18 14:12 012.pub
```

リストのディレクトリの下にあるファイルとサブディレクトリの詳細情報を表示します。

```
sftp> ls -l
-rwxrwxrwx    1 1        1             301 Dec 18 14:11 010.pub
-rwxrwxrwx    1 1        1             301 Dec 18 14:12 011.pub
-rwxrwxrwx    1 1        1             301 Dec 18 14:12 012.pub
```

🕮 **メモ：**

出力形式は、SSH サーバ装置モデルによって異なります。

5.2.12 mkdir

Syntax

mkdir *remote-path*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path: SFTP サーバのディレクトリ名を指定します。

説明

mkdir コマンドは SFTP サーバ上にディレクトリを作成します。

例

SFTP サーバ上にディレクトリを作成します。

sftp> mkdir test

5.2.13 put

Syntax

put *local-file* [*remote-file*]

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

local-file: ローカルファイルの名前を指定します。

remote-file: SFTP サーバの名前を指定します。指定しない場合、ファイルはローカルファイルと同一の名前で保存されます。

説明

put コマンドは SFTP サーバにローカルファイルをアップロードします。

例

SFTP サーバにローカルファイル startup.bak をアップロードし、startup01.bak として保存します。

sftp> put startup.bak startup01.bak

```
Uploading startup.bak to /startup01.bak
startup01.bak                                 100% 1424     1.4KB/s   00:00
```

5.2.14 pwd

Syntax

pwd

View

SFTP client view

定義済みユーザロール

network-admin

説明

pwd コマンドは SFTP サーバの現在の作業ディレクトリを表示します。

例

SFTP サーバの現在の作業ディレクトリを表示します。

sftp> pwd

```
Remote working directory: /
```

出力では、現在の作業ディレクトリはルートディレクトリであることを示します。

5.2.15 quit

Syntax

quit

View

SFTP client view

定義済みユーザロール

network-admin

説明

quit コマンドは SFTP サーバとの通信を終了し、user view に戻ります。

このコマンドは **bye** コマンド、**exit** コマンドと同一です。

例

SFTP サーバとの通信を終了し、user view に戻ります。

sftp> quit

<AP>

5.2.16 remove

Syntax

remove *remote-file*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-file: ファイルを指定します。

説明

remove コマンドは SFTP サーバからファイルを削除します。

このコマンドは **delete** コマンドと同一です。

例

SFTP サーバからファイル temp.c を削除します。

sftp> remove temp.c

```
Removing /temp.c
```

5.2.17 rename

Syntax

rename *old-name new-name*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

old-name: 既存のファイルあるいはディレクトリの名前を指定します。

new-name: 新しいファイルあるいはディレクトリの名前を指定します。

説明

rename コマンドは SFTP サーバのファイルあるいはディレクトリの名前を変更します。

例

SFTP サーバのファイルの名前を temp1.c から temp2.c に変更します。

sftp> dir

```
aa.pub  temp1.c
```

sftp> rename temp1.c temp2.c

sftp> dir

```
aa.pub  temp2.c
```

5.2.18 rmdir

Syntax

rmdir *remote-path*

View

SFTP client view

定義済みユーザロール

network-admin

パラメータ

remote-path: ディレクトリを指定します。

説明

rmdir コマンドは SFTP サーバからディレクトリを削除します。

例

SFTP サーバの現在のディレクトリの下のサブディレクトリ temp1 を削除します。

sftp> rmdir temp1

5.2.19 scp

Syntax

scp *server* [*port-numbe*r] { get | put } *source-file-name*

[*destination-file-name*] [identity-key { dsa | ecdsa-sha2-nistp256 |

ecdsa-sha2-nistp384 | rsa | { x509v3-ecdsa-sha2-nistp256 |

x509v3-ecdsa-sha2-nistp384 } pki-domain *domain-name* } | prefer-compress

zlib | prefer-ctos-cipher { 3des-cbc | aes128-cbc | aes128-ctr | aes128-gcm

| aes192-ctr | aes256-cbc | aes256-ctr | aes256-gcm | des-cbc } |

prefer-ctos-hmac { md5 | md5-96 | sha1 | sha1-96 | sha2-256 | sha2-512 } |

prefer-kex { dh-group-exchange-sha1 | dh-group1-sha1 | dh-group14-sha1 |

ecdh-sha2-nistp256 | ecdh-sha2-nistp384 } | prefer-stoc-cipher { 3des-cbc

| aes128-cbc | aes128-ctr | aes128-gcm | aes192-ctr | aes256-cbc |

aes256-ctr | aes256-gcm | des-cbc } | prefer-stoc-hmac { md5 | md5-96 | sha1

| sha1-96 | sha2-256 | sha2-512 }] * [{ public-key *keyname* |

server-pki-domain *domain-name* } | source { *interface interface-type interface-number* |

ip *ip-address* }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv4 アドレスまたはホスト名 (大文字と小文字を区別しない 1 ～ 253 文字の文字列) でサーバを指定します。

port-number: サーバのポート番号を 1 ～ 65535 の範囲で指定します。デフォルトは 22 です。

get: ファイルをダウンロードします。

put: ファイルをアップロードします。

source-file-name: ソースファイルの名前を、大文字と小文字を区別する 1 ～ 255 文字の文字列で指定します。

destination-file-name: ターゲット ファイルの名前を、大文字と小文字を区別する 1 ～ 255 文字の文字列で指定します。この引数を指定しない場合、ターゲット ファイルはソース ファイルと同じファイル名を使用します。

identity-key: クライアントの公開鍵認証のための公開鍵アルゴリズムを指定します。

デフォルトは DSA です。サーバが公開鍵認証を使用する場合は、このキーワードを指定する必要があります。クライアントは、指定されたアルゴリズムに関連付けられたローカル秘密キーを使用して、デジタル署名または証明書を生成します。

- dsa: 公開鍵アルゴリズム DSA を指定します。
- ecdsa-sha2-nistp256: 256 ビット鍵強度の ECDSA アルゴリズムを指定します。
- ecdsa-sha2-nistp384: ECDSA アルゴリズムを 384 ビット鍵強度で指定します。
- rsa: 公開鍵アルゴリズム RSA を指定します。
- x509v3-ecdsa-sha2-nistp256: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp256 を指定します。
- x509v3-ecdsa-sha2-nistp384: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp384 を指定します。
- pki-domain *domain-name*: クライアントの証明書の PKI ドメインを指定します。domain-name 引数は、大文字と小文字を区別しない 1 ～ 31 文字の文字列です。x509v3 公開キー アルゴリズムを使用する場合、クライアントが正しいローカル証明書を取得できるようにこのオプションを指定する必要があります。

prefer-compress: サーバとクライアント間のデータ圧縮に優先される圧縮アルゴリズムを指定します。デフォルトでは、圧縮はサポートされていません。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: 優先されるクライアントからサーバへの暗号化アルゴリズムを指定します。デフォルトは AES128-CTR です。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、DES-CBC、3DES-CBC、AES128-CBC、AES128-CTR、AES128-GCM、AES192-CTR、AES256-CBC、AES256-CTR、および AES256-GCM です。

- ・3des-cbc：暗号化アルゴリズム 3DES-CBC を指定します。
- ・aes128-cbc：暗号化アルゴリズム AES128-CBC を指定します。
- ・aes128-ctr：暗号化アルゴリズム AES128-CTR を指定します。
- ・aes128-gcm：暗号化アルゴリズム AES128-GCM を指定します。
- ・aes192-ctr：暗号化アルゴリズム AES192-CTR を指定します。
- ・aes256-cbc：暗号化アルゴリズム AES256-CBC を指定します。
- ・aes256-ctr：暗号化アルゴリズム AES256-CTR を指定します。
- ・aes256-gcm：暗号化アルゴリズム AES256-GCM を指定します。
- ・des-cbc：暗号化アルゴリズム DES-CBC を指定します。

prefer-ctos-hmac: 優先されるクライアントからサーバへの HMAC アルゴリズムを指定します。デフォルトは SHA2-256 です。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、MD5、MD5-96、SHA1、SHA1-96、SHA2-256、SHA2-512 です。

- ・ md5: HMAC アルゴリズム HMAC-MD5 を指定します。
- ・ md5-96: HMAC アルゴリズム HMAC-MD5-96 を指定します。
- ・ sha1: HMAC アルゴリズム HMAC-SHA1 を指定します。
- ・ sha1-96: HMAC アルゴリズム HMAC-SHA1-96 を指定します。
- ・ sha2-256: HMAC アルゴリズム HMAC-SHA2-256 を指定します。

- ・ sha2-512: HMAC アルゴリズム HMAC-SHA2-512 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。デフォルトは ecdh-sha2-nistp256 です。サポートされるアルゴリズムは、セキュリティ強度と計算時間の昇順で、diffie-hellman-group-exchange-sha1 、diffie-hellman-group1-sha1 、diffie-hellman-group14-sha1、ecdh-sha2-nistp256、そして ecdh-sha2-nistp384 です。

- dh-group-exchange-sha1: キー交換アルゴリズム
- diffie-hellman-group-exchange-sha1 を指定します。
- dh-group1-sha1: 鍵交換アルゴリズム diffie-hellman-group1-sha1 を指定します。
- dh-group14-sha1: 鍵交換アルゴリズム diffie-hellman-group14-sha1 を指定します。
- ecdh-sha2-nistp256: 鍵交換アルゴリズム ecdh-sha2-nistp256 を指定します。
- ecdh-sha2-nistp384: 鍵交換アルゴリズム ecdh-sha2-nistp384 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先暗号化アルゴリズムを指定します。デフォルトは AES128-CTR です。サポートされるアルゴリズムは、クライアントからサーバへの暗号化アルゴリズムと同じです (prefer-ctos-cipher キーワードを参照)。

prefer-stoc-hmac: サーバからクライアントへの優先 HMAC アルゴリズムを指定します。デフォルトは SHA2-256 です。サポートされるアルゴリズムは、クライアントからサーバへの HMAC アルゴリズムと同じです (prefer-ctos-hmac キーワードを参照)。

public-key *keyname*: クライアントがサーバを認証するために使用するサーバのホスト公開キーを指定します。keyname 引数は、大文字と小文字を区別しない 1 ～ 64 文字の文字列です。

server-pki-domain *domain-name*: サーバの証明書を検証するための PKI ドメインを指定します。domain-name 引数は、PKI ドメイン名を表します。大文字と小文字は区別されない 1 ～ 31 文字の文字列です。無効な文字は、チルダ (~)、アスタリスク (*)、バックスラッシュ (¥)、縦棒 (|)、コロン (:)、ドット (.)、山括弧 (< >)、引用符 (")、およびアポストロフィ (')。

source: SCP パケットの送信元 IPv4 アドレスまたは送信元インタフェースを指定します。デフォルトでは、デバイスはルーティング エントリの出力インタフェースのプライマリ IPv4 アドレスを SCP パケットの送信元アドレスとして使用します。SCP 接続を確実に成功させるためのベスト プラクティスとして、ループバック インタフェースを送信元インタフェースとして指定するか、ループバック インタフェースの IPv4 アドレスを送信元アドレスとして指定します。

- interface *interface-type interface-number*: 送信元インタフェースをタイプと番号で指定します。このインタフェースの IPv4 アドレスは、SCP パケットの送信元 IPv4 アドレスです。
- ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

scp を使用して、IPv4 SCP サーバへの接続を確立し、サーバとファイルを転送します。

クライアントが証明書認証を使用する場合、クライアントはサーバの証明書を検証する必要があります。

クライアントがサーバの証明書を正しく取得するには、server-pki-domain domain-name option を使用して、クライアント上でサーバの PKI ドメインを指定します。

クライアントは、指定された PKI ドメインに保存されている CA 証明書を使用してサーバの証明書を検証するため、認証前にサーバの公開キーを保存する必要はありません。

サーバの PKI ドメインを指定しない場合、クライアントは独自の証明書の PKI ドメインを使用してサーバの証明書を検証します。

SCP サーバが H3C デバイスの場合、SCP クライアントで destination-file-name 引数を使用して、ファイル パスの有無にかかわらずターゲット ファイル名を指定できます。

- 対象ファイル名をファイルパスを省略して指定する – SCP クライアントは、サーバからソース ファイルを SCP クライアントの現在の作業ディレクトリにダウンロードするか、ソース ファイルをサーバの現在の作業ディレクトリにアップロードして、そのファイルの名前をターゲット ファイル名に変更します。たとえば、ファイル remote.bin をサーバからクライアントの現在の作業ディレクトリにダウンロードし、その名前を local.bin に変更するには、destination-file-name 引数を local.bin として指定できます。
- 対象ファイル名をファイルパスで指定 – SCP クライアントは、サーバからソースファイルを SCP クライアントの指定されたファイル パスにダウンロードするか、ソース ファイルをサーバの指定されたファイル パスにアップロードして、そのファイルの名前をターゲット ファイル名に変更します。たとえば、ファイル remote.bin をサーバからクライアントのパス flash:/logfile にダウンロードし、その名前を local.bin に変更するには、destination-file-name 引数を flash:/logfile/local.bin または logfile/local.bin として指定できます。

例

SCP クライアントを SCP サーバ 200.1.1.1 に接続します。サーバの公開鍵を svkey として指定し、サーバからファイル abc.txt をダウンロードします。SCP クライアントは公開鍵認証を使用します。次のアルゴリズムを使用します。

- Preferred key exchange algorithm: dh-group14-sha1.
- Preferred server-to-client encryption algorithm: aes128-cbc.
- Preferred client-to-server HMAC algorithm: sha1.
- Preferred server-to-client HMAC algorithm: sha1-96.
- Preferred compression algorithm: zlib.

```
<AP> scp 200.1.1.1 get abc.txt prefer-kex dh-group14-sha1 prefer-stoc-cipher
aes128-cbc prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib
public-key
```

```
svkey
Username:
```

5.2.20 sftp

Syntax

sftp server [port-number] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** domain-name } | **prefer-compress** **zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | prefer-ctos-hmac { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | dh-group14-sha1 | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { 3des-cbc | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** dscp-value | { **public-key** keyname | **server-pki-domain** domain-name } | **source** { **interface** interface-type interface-number | **ip** ip-address }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv4 アドレスあるいはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

identity-key: クライアントの公開鍵アルゴリズムを指定します。サーバが公開鍵認証を使用する場合、指定する必要があります。クライアントはアルゴリズムに関連したローカル秘密鍵を使用してデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **ecdsa-sha2-nistp256**: 256-bit key strength の ECDSA アルゴリズムを指定します。
- **ecdsa-sha2-nistp384**: 384-bit key strength の ECDSA アルゴリズムを指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。

- **x509v3-ecdsa-sha2-nistp256**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp256. を指定します。
- **x509v3-ecdsa-sha2-nistp384**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp384 を指定します。
- **pki-domain** domain-name: クライアントの証明書の PKI ドメインを指定します。domain-name 引数は、大文字と小文字を区別しない 1 ～ 31 文字の文字列です。x509v3 公開鍵アルゴリズムを使用する場合､クライアントが正しいローカル証明書を取得するには、このオプションを指定する必要があります。

prefer-compress: サーバとクライアント間で優先される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先される暗号化アルゴリズムを指定します。アルゴリズム **des-cbc**、**3des-cbc**、**aes128-cbc** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **3des-cbc**: 暗号化アルゴリズム 3des-cbc を指定します。
- **aes128-cbc**: 暗号化アルゴリズム aes128-cbc を指定します。
- **aes128-ctr**: 暗号化アルゴリズム AES128-CTR を指定します。
- **aes128-gcm**: 暗号化アルゴリズム AES128-GCM を指定します。
- **aes192-ctr**: 暗号化アルゴリズム AES192-CTR を指定します。
- **aes256-cbc**: 暗号化アルゴリズム AES256-CBC を指定します。
- **aes256-ctr**: 暗号化アルゴリズム AES256-CTR を指定します。
- **aes256-gcm**: 暗号化アルゴリズム AES256-GCM を指定します。
- **des-cbc**: 暗号化アルゴリズム des-cbc を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先される HMAC アルゴリズムを指定します。アルゴリズム **md5**、**md5-96**、**sha1**、**sha1-96** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **md5:** HMAC アルゴリズム hmac-md5 を指定します。
- **md5-96:** HMAC アルゴリズム hmac-md5-96 を指定します。
- **sha1:** HMAC アルゴリズム hmac-sha1 を指定します。
- **sha1-96:** HMAC アルゴリズム hmac-sha1-96 を指定します。
- **sha2-256**: HMAC アルゴリズム HMAC-SHA2-256 を指定します。
- **sha2-512**: HMAC アルゴリズム HMAC-SHA2-512 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。アルゴリズム **dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **dh-group-exchange-sha1**: 鍵交換アルゴリズム diffie-hellman-group-exchange-sha1 を指定します。
- **dh-group1-sha1**: 鍵交換アルゴリズム diffie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム diffie-hellman-group14-sha1 を指定します。
- **ecdh-sha2-nistp256**: 鍵交換アルゴリズム ecdh-sha2-nistp256 を指定します。
- **ecdh-sha2-nistp384**: 鍵交換アルゴリズム ecdh-sha2-nistp384 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先される暗号化アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-cipher** 暗号化アルゴリズムと同一にしてください。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-hmac** 暗号化アルゴリズムと同一にしてください。

dscp *dscp-value*: SFTP クライアントによって送信される IPv4 SFTP パケットの DSCP を指定します。設定範囲は 0〜63 です。デフォルトは 48 です。DSCP の値はパケットを送信するプライオリティに影響します。

public-key *keyname*: サーバを認証するためにクライアントが使用するサーバのホスト公開鍵を指定します。設定範囲は 1〜64 文字です。

server-pki-domain domain-name: サーバの証明書を検証するための PKI ドメインを指定します。domain-name 引数は、大文字と小文字を区別しない 1 〜 31 文字の文字列である PKI ドメイン名を表します。無効な文字は、チルダ (~)、アスタリスク (*)、バックスラッシュ (¥)、縦棒 (|)、コロン (:)、ドット (.)、山かっこ (< >)、引用符 (")、およびアポストロフィ (')。

source: SFTP パケットの送信元 IP アドレスあるいは送信元インタフェースを指定します。デフォルトで SFTP パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。SFTP 接続を正しく行うため、送信元インタフェースとしてループバックインタフェースを指定する、あるいは送信元 IPv4 アドレスとしてループバックインタフェースの IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは SFTP パケットの送信元 IPv4 アドレスです。
- **ip** *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

sftp コマンドは IPv4 SFTP サーバとの接続を確立し、SFTP client view に移行します。

公開鍵認証では、クライアントはデジタル認証のローカルプライベート鍵を取得する必要があります。

例

IPv4 SFTP サーバ 10.1.1.2 に SFP クライアントを接続し、サーバの公開鍵として svkey を指定します。SFTP クライアントは公開鍵認証を使用します。以下のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先される暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先される HMAC アルゴリズムは sha1 です。
- サーバからクライアントへの優先される HMAC アルゴリズムは sha1-96 です。
- サーバとクライアント間で優先される圧縮アルゴリズムは zlib です。

<AP> sftp 10.1.1.2 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc

prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey

5.2.21 sftp client source

Syntax

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

undo sftp client source

デフォルト

SFTP パケットの送信元 IP アドレスは設定されていません。SFTP パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。SFTP パケットは送信元アドレスとしてインタフェースのプライマリ IP アドレスを使用します。

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

sftp client source コマンドは SFTP パケットの送信元 IPv4 アドレスを指定します。

undo sftp client source コマンドはデフォルトに戻します。

このコマンドはすべての SFTP 接続に適用します。**sftp** コマンドで指定された送信元 IP アドレスは、現在の SFTP 接続のみ適用します。このコマンドと **sftp** コマンドの両方で送信元 IP アドレスが指定された場合、**sftp** コマンドで指定された送信元 IP アドレスが適用されます。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

SFTP パケットの送信元 IP アドレスとして 192.168.0.1 を指定します。

<AP> system-view

[AP] sftp client source ip 192.168.0.1

関連コマンド

display sftp client source

5.2.22 ssh client source

Syntax

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

undo ssh client source

デフォルト

SSH パケットの送信元 IP アドレスは設定されていません。SSH パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。

View

System view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。SSH パケットは送信元アドレスとしてインタフェースのプライマリ IP アドレスを使用します。

ip *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

ssh client source コマンドは Stelnet クライアントが送信する SSH パケットの送信元 IPv4 アドレスを指定します。

undo ssh client source コマンドはデフォルトに戻します。

このコマンドはすべての Stelnet 接続に適用します。**ssh2** コマンドで指定された送信元 IP アドレスは、現在の Stelnet 接続のみ適用します。このコマンドと **ssh2** コマンドの両方で送信元 IP アドレスが指定された場合、**ssh2** コマンドで指定された送信元 IP アドレスが適用されます。

このコマンドを複数実行した場合、最後に行われた設定が適用されます。

例

SSH パケットの送信元 IPv4 アドレスとして 192.168.0.1 を指定します。

<AP> system-view

[AP] ssh client source ip 192.168.0.1

関連コマンド

display ssh client source

5.2.23 ssh2

Syntax

ssh2 server [port-number] [**identity-key** { **dsa** | **ecdsa-sha2-nistp256** | **ecdsa-sha2-nistp384** | **rsa** | { **x509v3-ecdsa-sha2-nistp256** | **x509v3-ecdsa-sha2-nistp384** } **pki-domain** domain-name } | **prefer-compress** **zlib** | **prefer-ctos-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } | **prefer-kex** { **dh-group-exchange-sha1** | **dh-group1-sha1** | **dh-group14-sha1** | **ecdh-sha2-nistp256** | **ecdh-sha2-nistp384** } | **prefer-stoc-cipher** { **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes128-gcm** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **aes256-gcm** | **des-cbc** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }] * [**dscp** dscp-value | **escape** character | { **public-key** keyname | **server-pki-domain** domain-name } | **source** { **interface** interface-type interface-number | **ip** ip-address }] *

View

User view

定義済みユーザロール

network-admin

パラメータ

server: IPv4 アドレスあるいはホスト名でサーバを指定します。設定範囲は 1～253 文字です。大文字、小文字を区別しません。

port-number: サーバのポート番号を指定します。設定範囲は 1～65535 です。デフォルトは 22 です。

identity-key: クライアントの公開鍵アルゴリズムを指定します。サーバが公開鍵認証を使用する場合、指定する必要があります。クライアントはアルゴリズムに関連したローカル秘密鍵を使用してデジタル署名を作成します。

- **dsa**: 公開鍵アルゴリズム dsa を指定します。
- **ecdsa-sha2-nistp256**: 256-bit key strength の ECDSA アルゴリズムを指定します。

- **ecdsa-sha2-nistp384**: 384-bit key strength の ECDSA アルゴリズムを指定します。
- **rsa**: 公開鍵アルゴリズム rsa を指定します。
- **x509v3-ecdsa-sha2-nistp256**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp256. を指定します。
- **x509v3-ecdsa-sha2-nistp384**: 公開鍵アルゴリズム x509v3-ecdsa-sha2-nistp384 を指定します。
- **pki-domain** domain-name: クライアントの証明書の PKI ドメインを指定します。domain-name 引数は、大文字と小文字を区別しない 1 ～ 31 文字の文字列です。x509v3 公開鍵アルゴリズムを使用する場合､クライアントが正しいローカル証明書を取得するには、このオプションを指定する必要があります。

prefer-compress: サーバとクライアント間で優先される圧縮アルゴリズムを指定します。

zlib: 圧縮アルゴリズム zlib を指定します。

prefer-ctos-cipher: クライアントからサーバへの優先される暗号化アルゴリズムを指定します。アルゴリズム **des-cbc**、**3des-cbc**、**aes128-cbc** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **3des-cbc**: 暗号化アルゴリズム 3des-cbc を指定します。
- **aes128-cbc**: 暗号化アルゴリズム aes128-cbc を指定します。
- **aes128-ctr**: 暗号化アルゴリズム AES128-CTR を指定します。
- **aes128-gcm**: 暗号化アルゴリズム AES128-GCM を指定します。
- **aes192-ctr**: 暗号化アルゴリズム AES192-CTR を指定します。
- **aes256-cbc**: 暗号化アルゴリズム AES256-CBC を指定します。
- **aes256-ctr**: 暗号化アルゴリズム AES256-CTR を指定します。
- **aes256-gcm**: 暗号化アルゴリズム AES256-GCM を指定します
- **des-cbc**: 暗号化アルゴリズム des-cbc を指定します。

prefer-ctos-hmac: クライアントからサーバへの優先される HMAC アルゴリズムを指定します。アルゴリズム **md5**、**md5-96**、**sha1**、**sha1-96** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

- **md5:** HMAC アルゴリズム hmac-md5 を指定します。
- **md5-96:** HMAC アルゴリズム hmac-md5-96 を指定します。
- **sha1:** HMAC アルゴリズム hmac-sha1 を指定します。
- **sha1-96:** HMAC アルゴリズム hmac-sha1-96 を指定します。
- **sha2-256**: HMAC アルゴリズム HMAC-SHA2-256 を指定します。
- **sha2-512**: HMAC アルゴリズム HMAC-SHA2-512 を指定します。

prefer-kex: 優先される鍵交換アルゴリズムを指定します。アルゴリズム **dh-group-exchange-sha1**、**dh-group1-sha1**、**dh-group14-sha1** の順番でセキュリティの強度が強くなり、計算時間が長くなります。

dh-group-exchange-sha1: 鍵交換アルゴリズム diffie-hellman-group-exchange-sha1 を指定します。

- **dh-group1-sha1**: 鍵交換アルゴリズム diffie-hellman-group1-sha1 を指定します。
- **dh-group14-sha1**: 鍵交換アルゴリズム diffie-hellman-group14-sha1 を指定します。

- **ecdh-sha2-nistp256**: 鍵交換アルゴリズム ecdh-sha2-nistp256 を指定します。
- **ecdh-sha2-nistp384**: 鍵交換アルゴリズム ecdh-sha2-nistp384 を指定します。

prefer-stoc-cipher: サーバからクライアントへの優先される暗号化アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-cipher** 暗号化アルゴリズムと同一にしてください。

prefer-stoc-hmac: サーバからクライアントへの優先される HMAC アルゴリズムを指定します。サポートするアルゴリズムは **prefer-ctos-hmac** 暗号化アルゴリズムと同一にしてください。

dscp *dscp-value*: IPv4 SSH パケットの DSCP を指定します。設定範囲は 0〜63 です。デフォルトは 48 です。DSCP の値はパケットを送信するプライオリティに影響します。

escape *character*: Stelnet 接続を切断するための文字を指定します。デフォルトはチルダ（~）です。

public-key *keyname*: サーバのホスト公開鍵を指定します。サーバを認証するために使用します。設定範囲は 1〜64 です。大文字、小文字を区別しません。

server-pki-domain domain-name: サーバの証明書を検証するための PKI ドメインを指定します。domain-name 引数は、大文字と小文字を区別しない 1 〜 31 文字の文字列である PKI ドメイン名を表します。無効な文字は、チルダ (~)、アスタリスク (*)、バックスラッシュ (¥)、縦棒 (|)、コロン (:)、ドット (.)、山かっこ (< >)、引用符 (")、およびアポストロフィ（ '）。

source: SSH パケットの送信元 IP アドレスあるいは送信元インタフェースを指定します。デフォルトで SSH パケットは送信元アドレスとして、ルーティングエントリで指定された送信インタフェースのプライマリ IP アドレスを使用します。Stelnet 接続を正しく行うため、送信元インタフェースとしてループバックインタフェースを指定する、あるいは送信元 IPv4 アドレスとしてループバックインタフェースの IPv4 アドレスを指定します。

- **interface** *interface-type interface-number*: 送信元インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは SSH パケットの送信元 IP アドレスです。
- **ip** *ip-address*: 送信元 IPv4 アドレスを指定します。

説明

ssh2 コマンドは IPv4 Stelnet サーバとの接続を確立します。

escape *character* パラメータとドット（.）の組み合わせは、エスケープシーケンスとして働きます。このエスケープシーケンスは、一般に、サーバが再起動や例外的な挙動をするときに SSH 接続を素早く切断します。

エスケープシーケンスを適用するには、ラインのその最初に入力しなければなりません。ラインに他の文字を入力したり、操作を実行した場合、次のラインにエスケープシーケンスを入力してください。

escape *character* パラメータにはデフォルトの（~）を使用することを推奨します。SSH ユーザ名として別の文字を使用しないでください。

例

IPv4 Stelnet サーバ 3.3.3.3 へ接続を確立し、サーバの公開鍵として svkey を指定します。Stelnet クライアントは公開鍵認証を使用します。**escape** *character* として（$）を指定します。以下のアルゴリズムを使用します。

- 優先される鍵交換アルゴリズムは dh-group14-sha1 です。
- サーバからクライアントへの優先される暗号化アルゴリズムは aes128-cbc です。
- クライアントからサーバへの優先される HMAC アルゴリズムは sha1 です。
- サーバからクライアントへの優先される HMAC アルゴリズムは sha1-96 です。
- サーバとクライアント間で優先される圧縮アルゴリズムは zlib です。

<AP> ssh2 3.3.3.3 prefer-kex dh-group14-sha1 prefer-stoc-cipher aes128-cbc

prefer-ctos-hmac sha1 prefer-stoc-hmac sha1-96 prefer-compress zlib public-key svkey escape $

目次

このセクションのページは **13-x-x** です。

6 章 パスワード管理 6-1
6.1 パスワード管理設定コマンド 6-1
6.1.1 display password-control 6-1
6.1.2 display password-control blacklist 6-4
6.1.3 password-control { composition | history | length } enable 6-6
6.1.4 password-control aging 6-7
6.1.5 password-control alert-before-expire 6-9
6.1.6 password-control change-password first-login enable 6-9
6.1.7 password-control complexity 6-10
6.1.8 password-control composition 6-12
6.1.9 password-control enable 6-14
6.1.10 password-control expired-user-login 6-15
6.1.11 password-control history 6-16
6.1.12 password-control length 6-17
6.1.13 password-control login idle-time 6-19
6.1.14 password-control login-attempt 6-20
6.1.15 password-control super aging 6-24
6.1.16 password-control super composition 6-25
6.1.17 password-control super length 6-26
6.1.18 password-control update-interval 6-27
6.1.19 reset password-control blacklist 6-28
6.1.20 reset password-control history-record 6-28

6章 パスワード管理

6.1 パスワード管理設定コマンド

6.1.1 display password-control

Syntax

display password-control [**super**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

super: super パスワードのパスワード管理の情報を表示します。指定しない場合、グローバルのパスワード管理の設定を表示します。

説明

display password-control コマンドはパスワード管理の設定を表示します。

Enabled と表示されているコマンドでも、**password-control enable** コマンドの有効化が必要な機能は、**Enabled** と表示されている状態でも動作しません。

例

グローバルのパスワード管理の設定を表示します。

<AP> display password-control

```
Global password control configurations:
 Password control:                  Enabled (device management users)
                                  Enabled (network access users)
 Password aging:                    Enabled (90 days)
 Password length:                   Enabled (10 characters)
 Password composition:               Enabled (1 types, 1 characters per type)
 Password history:                  Enabled (max history records:4)
 Early notice on password expiration:  7 days
 User authentication timeout:          600 seconds
 Maximum login attempts:              3
 Action for exceeding login attempts:  Lock user for 1 minutes
```

```
Minimum interval between two updates: 24 hours
User account idle time:             90 days
Logins with aged password:          3 times in 30 days
Password complexity:                Disabled (username checking)
                                    Disabled (repeated characters checking)
Password change:                    Enabled (first login)
```

super パスワードのパスワード管理の設定を表示します。

<AP> display password-control super

```
Super password control configurations:
Password aging:                     Enabled (90 days)
Password length:                    Enabled (10 characters)
Password composition:               Enabled (1 types, 1 characters per type)
```

表 7-1 コマンド出力

フィールド	説明
Password control	パスワード管理機能が有効かどうかを示します。
Password aging	パスワードの有効期限の設定が有効かどうかを示します。有効である場合、有効期限が表示されます。
Password length	最小パスワード長の設定が有効かどうかを示します。有効である場合、設定を表示します。
Password composition	パスワード構成ポリシー機能が有効かどうかを示します。有効である場合、設定を表示します。
Password history	パスワード履歴機能が有効かどうかを示します。有効である場合、設定を表示します。
Early notice on password expiration	ユーザのパスワードの有効期限が終了する前に、ユーザに通知するまでの日数です。
Maximum login attempts	FTPユーザとVTYユーザがログインできる最大試行回数です。
Action for exceeding login attempts	ユーザが試行回数後にログインに失敗したときのアクションです。 ● **Lock**—アカウントを永続的にロックします。 ● **Lock user for x minutes**—アカウントをx分間ロックします。フィールドは、ロックタイマの期限が切れた後、アカウントが再度ログイン試行の最大回数に失敗するたびに、アカウントのロック期間が増加することを示します。フィールドは、最大ロック期間を示します。 ● **Unlock**—アカウントをロックしません。
Minimum interval between two updates	パスワードアップデートの最小間隔です。

フィールド	説明
Login with aged password	パスワードの有効期限後、ユーザがログインできる最大日時と最大回数です。
Password complexity	次のパスワード複雑性チェック（ユーザ名チェックと繰り返し文字チェック）を有効にするかどうかを示します。
Password change	初回ログイン時のパスワード変更機能の状態を示します。 ● **Enabled (first login)**— 初回ログイン時のパスワード変更機能が有効です。 ● **Disabled (first login)**— 初回ログイン時のパスワード変更機能が無効です。 ● **Enabled (mandatory weak password change)** —必須の弱いパスワード変更機能が有効です。 ● **Disabled (mandatory weak password change)** —必須の弱いパスワード変更機能が無効です。
User information in blacklist	パスワード制御ブラックリストに追加されたユーザ情報項目です。 ● **Username-only**—パスワード制御ブラックリストにユーザ名のみが追加されます。 ● **Username and IP**—ユーザ名とIPアドレスの両方がパスワード制御ブラックリストに追加されます。
All line	すべてのユーザ回線タイプのパスワード制御ブラックリスト機能のステータスです。 ● **Enabled (all line blacklist)** —全回線ブラックリストが有効です。 ● **Disabled (all line blacklist)** —全回線ブラックリストが無効です。

6.1.2 display password-control blacklist

Syntax

display password-control blacklist [**user-name** *user-name* | **ip** *ipv4-address*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

user-name *user-name*: ユーザ名を指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。

ip *ipv4-address*: ユーザの IPv4 アドレスを指定します。

説明

display password-control blacklist コマンドはパスワード管理ブラックリストの情報を表示します。

パラメータを指定しない場合、パスワード管理ブラックリストのすべてのユーザの情報を表示します。

コンソールポートを経由してアクセスしたユーザが認証に失敗すると、そのユーザアカウントがパスワード制御ブラックリストに追加されます。FTP や VTY ユーザが認証に失敗すると、その IP アドレスおよびユーザアカウントがパスワード制御ブラックリストに追加されます。**display password-control blacklist** コマンドを使用して、ブラックリストに掲載されたユーザに関する情報を表示できます。

装置は、次の条件が両方とも満たされた場合に、ユーザアカウントの IP アドレスごとにブラックリストエントリを作成します。

- ユーザ名と IP アドレスの両方がパスワード制御ブラックリストに追加されます。
- ユーザは同じユーザアカウントを使用して、異なる IP アドレスから装置にログインし、ログインに失敗します。

ユーザアカウントのブラックリストエントリの最大数に達すると、そのユーザアカウントの新しい IP アドレスのブラックリストエントリによって、そのユーザアカウントの最も古いブラックリストエントリが上書きされます。

例

パスワード管理ブラックリストのユーザの情報を表示します。

<AP> display password-control blacklist

```
Blacklist items matched: 2.
```

```
Username                 IP address          Login failures   Lock flag
abcd                     169::168:34:1       4                lock
admin                    192.168.34.1        1                unlock
```

表 7-2 コマンド出力

フィールド	説明
Per-user blacklist limit	ユーザーアカウントのブラックリストエントリの最大数です。
Blacklist items matched	ブラックリストのユーザ数です。
IP address	ユーザのIPアドレスです。
Login failures	ログイン失敗回数です。
Lock flag	ユーザログインの禁止が行われているかどうかを示します。IPアドレスを持つユーザの場合、ユーザアカウントとIPアドレスの両方がロックされます。 IPアドレスを持たないユーザの場合は、ユーザアカウントだけがロックされます。ユーザは、このユーザアカウントを使用してコンソール回線経由でログインすることはできません。 ● **unlock**—禁止されていません。 ● **lock**— **password-control login-attempt**コマンドによって一時的あるいは永久に禁止されています。

6.1.3 password-control { composition | history | length } enable

Syntax

password-control { **composition** | **history** | **length** } **enable**

undo password-control { **composition** | **history** | **length** } **enable**

デフォルト

パスワード管理機能はすべて（**aging**、**composition**、**history**、**length**）有効です。

View

System view

定義済みユーザロール

network-admin

パラメータ

composition: パスワード構成ポリシー機能を有効にします。

history: パスワード履歴機能を有効にします。

length: 最小パスワード長の設定を有効にします。

説明

password-control { **composition | history | length** } **enable** コマンドはパスワード管理機能（有効期限、パスワード構成ポリシー、パスワード履歴、最小パスワード長の機能）を有効にします。

undo password-control { **composition | history | length** } **enable** コマンドはパスワード管理機能を無効にします。

グローバルパスワード制御機能（**password-control enable** コマンド）が有効であるかどうかに関係なく、パスワード構成の制限および最小パスワード長制限がデフォルトで有効になります。デフォルトでは、パスワード構成ポリシーと最小パスワード長は次のとおりです。

- パスワードには、2 つ以上の文字タイプと、各タイプにつき 1 つ以上の文字を含める必要があります。
- パスワードは 10 文字以上にする必要があります。

装置管理ユーザのパスワードがハッシュ形式の場合、次の要件を満たしていても、パスワードに対する制限設定は有効になりません。

- グローバルパスワード制御が有効
- パスワード制限機能が有効

undo password-control history enable コマンドを実行した後、システムは新しいパスワードと履歴パスワードを比較しませんが、履歴パスワードの記録は停止しません。ユーザの履歴パスワードレコードの数が **password-control history** コマンドで設定された

最大数に達すると、最新の履歴レコードによって最も古い履歴レコードが上書きされます。

例

グローバルパスワード管理機能を有効にします。

<AP> system-view

[AP] password-control enable

パスワード構成ポリシー機能を有効にします。

[AP] password-control composition enable

パスワードの有効期限の機能を有効にします。

[AP] password-control aging enable

最小パスワード長の設定を有効にします。

[AP] password-control length enable

パスワード履歴の機能を有効にします。

[AP] password-control history enable

関連コマンド

- **display password-control**
- **password-control enable**

6.1.4 password-control aging

Syntax

password-control aging *aging-time*

undo password-control aging

デフォルト

パスワードの有効期限は 90 日です。ユーザグループのパスワードの有効期限はグローバルの設定と同一です。ローカルユーザのパスワードの有効期限はローカルユーザが所属しているユーザグループのパスワードの有効期限と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

aging-time: パスワードの有効期限を指定します。設定範囲は 1～365 日です。

説明

password-control aging コマンドはパスワードの有効期限を設定します。

undo password-control aging コマンドはデフォルトに戻します。

パスワードの有効期限は各 view に依存します。

- system view のパスワードの有効期限はグローバルであり、すべてのユーザグループに適用します。
- user group view のパスワードの有効期限はユーザグループのすべてのローカルユーザに適用します。
- local user view のパスワードの有効期限はローカルユーザのみに適用します。

パスワードの有効期限は小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のパスワードの有効期限を使用します。

- ローカルユーザにパスワードの有効期限が設定されていない場合、システムはローカルユーザが所属しているユーザグループのパスワードの有効期限を使用します。
- ユーザグループにパスワードの有効期限が設定されていない場合、システムはグローバルのパスワードの有効期限を使用します。

例

グローバルのパスワードの有効期限を 80 日に設定します。

<AP> system-view

[AP] password-control aging 80

ユーザグループ **test** のパスワードの有効期限を 90 日に設定します。

[AP] user-group test

[AP-ugroup-test] password-control aging 90

[AP-ugroup-test] quit

装置管理ユーザ **abc** のパスワードの有効期限を 100 日に設定します。

[AP] local-user abc class manage

[AP-luser-manage-abc] password-control aging 100

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**
- **password-control aging enable**

6.1.5 password-control alert-before-expire

Syntax

password-control alert-before-expire *alert-time*

undo password-control alert-before-expire

デフォルト

7 日

View

System view

定義済みユーザロール

network-admin

パラメータ

alert-time: ユーザのパスワードの有効期限が終了する前にユーザに通知するまでの日数を指定します。設定範囲は 1～30 日です。

説明

password-control alert-before-expire コマンドはユーザのパスワードの有効期限が終了する前に、ユーザに通知するまでの日数を設定します。

undo password-control alert-before-expire コマンドはデフォルトに戻します。

このコマンドは FTP ユーザ以外のユーザに適用されます。FTP ユーザは、管理者によってのみパスワードを変更することができます。

例

ユーザのパスワードの有効期限が終了する前に、ユーザに通知するまでの日数を 10 日に設定します。

<AP> system-view

[AP] password-control alert-before-expire 10

関連コマンド

display password-control

6.1.6 password-control change-password first-login enable

Syntax

password-control change-password first-login enable

undo password-control change-password first-login enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

password-control change-password first-login enable コマンドは、初回ログイン時のパスワード変更機能を有効にします。

undo password-control change-password first-login enable コマンドは、初回ログイン時のパスワード変更機能を無効にします。

初回ログイン時のパスワード変更機能を有効にするには、**password-control enable** コマンドと **password-control change-password first-login enable** コマンドの両方を設定する必要があります。

例

初回ログイン時のパスワード変更機能を有効に設定します。

<AP> system-view

[AP] password-control change-password first-login enable

関連コマンド

- **display password-control**
- **password-control enable**

6.1.7 password-control complexity

Syntax

password-control complexity { **same-character** | **user-name** } **check**

undo password-control complexity { **same-character** | **user-name** } **check**

デフォルト

ユーザグループのパスワードの複雑性のポリシーはグローバルの設定と同一です。ローカルユーザのパスワードの複雑性のポリシーはローカルユーザが所属しているユーザグループのパスワードの複雑性のポリシーと同一です。

グローバルのパスワードの複雑性のポリシーは、**user-name check** は有効、**same-character check** は無効です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

same-character: パスワードに文字あるいは数字が 3 回以上連続して続くことを禁止します。たとえば、パスワード **aaabc** はポリシーに適合しません。

user-name: パスワードにユーザ名あるいはユーザ名の逆の順番を含むことを禁止します。

- ユーザ名が **123** の場合、**abc 123** や **321 df** などのパスワードはポリシーに適合しません。
- ユーザ名が **12345** の場合、**123** などのパスワードはポリシーに適合しません。

password-control enable コマンドを設定していなくても、本コマンドが有効な場合には有効になります。

説明

password-control complexity コマンドはパスワードの複雑性のポリシーを設定します。

undo password-control complexity コマンドはパスワードの複雑性のポリシーを削除します。

パスワードの複雑性のポリシーは各 view に依存します。

- system view のパスワードの複雑性のポリシーはグローバルであり、すべてのユーザグループに適用します。
- user group view のパスワードの複雑性のポリシーはユーザグループのすべてのローカルユーザに適用します。
- local user view のパスワードの複雑性のポリシーはローカルユーザのみに適用します。

パスワードの複雑性のポリシーは小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のパスワードの複雑性のポリシーを使用します。

- ローカルユーザにパスワードの複雑性のポリシーが設定されていない場合、システムはローカルユーザが所属しているユーザグループのパスワードの複雑性のポリシーを使用します。
- ユーザグループにパスワードの複雑性のポリシーが設定されていない場合、システムはグローバルのパスワードの複雑性のポリシーを使用します。

パスワード内のユーザ名の有無の確認と、パスワードの文字の反復回数の確認の両方を有効にすることができます。

例

パスワード内のユーザ名の有無の確認、あるいはパスワードの文字の反復回数の確認を禁止するパスワードの複雑性のポリシーを設定します。

<AP> system-view

[AP] password-control complexity user-name check

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**

6.1.8 password-control composition

Syntax

password-control composition type-number *type-number* [**type-length** *type-length*]

undo password-control composition

デフォルト

グローバルのパスワード構成ポリシーは、少なくとも 2 種類の文字タイプと、各タイプに 1 文字以上を含む必要があります。

ユーザグループのパスワード構成ポリシーはグローバルの設定と同一です。ローカルユーザのパスワード構成ポリシーはローカルユーザが所属しているユーザグループのパスワード構成ポリシーと同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

type-number *type-number*: パスワードに含まれる文字タイプの最小数を指定します。設定範囲は 1~4 です。

type-length *type-length*: パスワードの各タイプの最小文字数を指定します。設定範囲は 1～63 です。

説明

password-control composition コマンドはパスワード構成ポリシーを設定します。

undo password-control composition コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

パスワード構成ポリシーは各 view に依存します。

- system view のパスワード構成ポリシーはグローバルであり、すべてのユーザグループに適用します。
- user group view のパスワード構成ポリシーはユーザグループのすべてのローカルユーザに適用します。
- local user view のパスワード構成ポリシーはローカルユーザのみに適用します。

パスワード構成ポリシーは小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のパスワード構成ポリシーを使用します。

- ローカルユーザにパスワード構成ポリシーが設定されていない場合、システムはローカルユーザが所属しているユーザグループのパスワード構成ポリシーを使用します。
- ユーザグループにパスワード構成ポリシーが設定されていない場合、システムはグローバルのパスワード構成ポリシーを使用します。

文字タイプの最小数と各タイプの最小文字数はパスワードの最大長より小さくする必要があります。

例

すべてのパスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

<AP> system-view

[AP] password-control composition type-number 4 type-length 5

ユーザグループ **test** のパスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

[AP] user-group test

[AP-ugroup-test] password-control composition type-number 4 type-length 5

[AP-ugroup-test] quit

装置管理ユーザ **abc** のパスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

[AP] local-user abc class manage

[AP-luser-manage-abc] password-control composition type-number 4 type-length 5

関連コマンド

- **display local-user**
- **display password-control**

- **display user-group**
- **password-control composition enable**

6.1.9 password-control enable

Syntax

password-control enable [**network-class**]

undo password-control enable [**network-class**]

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

network-class: ネットワークアクセスユーザのグローバルパスワード制御を有効にします。このキーワードを指定しない場合、コマンドはデバイス管理ユーザのグローバルパスワード制御を有効にします。

説明

password-control enable コマンドはグローバルでパスワード管理機能を有効にします。

undo password-control enable コマンドはグローバルでパスワード管理機能を無効にします。

グローバルでパスワード管理機能を有効にしたのち、指定したパスワード管理機能が適用されます。

グローバルでパスワード管理機能を有効にしたのち、対応する **display** コマンドを使用して装置管理ユーザのパスワード設定と super パスワードの設定を表示することはできません。ネットワークアクセスユーザのパスワード設定が表示されます。装置管理ユーザの設定された初期パスワードは少なくとも 4 種類の文字を含む必要があります。

デバイス管理ユーザのすべてのパスワード制御機能を設定できます。

ネットワークアクセスユーザの場合、次のパスワード制御機能のみを設定できます。

- パスワード複雑性チェックポリシー
- パスワード構成ポリシー
- パスワードの最小長
- パスワードの最小更新間隔
- 各ユーザの履歴パスワードレコードの最大数

装置管理ユーザの場合、パスワード構成の制限、最小パスワード長の制限、およびユーザ名チェックは、グローバルパスワード制御機能とは無関係です。その他のパスワード制御機能は、グローバルパスワード制御機能が有効になった後にのみ有効になります。

ネットワークアクセスユーザの場合、すべてのパスワード制御機能は、グローバルパスワード制御機能が有効になってから有効になります。

グローバルパスワード制御機能を有効にした後、ローカルユーザに設定するパスワードには、最低 4 つの異なる文字を含める必要があります。

装置管理ユーザに対してグローバルパスワード制御機能を有効にすると、対応する **display** コマンドを使用して装置管理ユーザのパスワードおよびスーパーパスワード設定を表示できなくなります。

ネットワークアクセスユーザに対してグローバルパスワード制御機能を有効にすると、対応する **display** コマンドを使用してネットワークアクセスユーザのパスワード設定を表示できなくなります。

例

グローバルでパスワード管理機能を有効にします。

<AP> system-view

[AP] password-control enable

#ネットワークアクセスユーザに対してパスワード制御機能をグローバルに有効にします。

< AP > system-view

[AP] password-control enable network-class

関連コマンド

- **display password-control**
- **password-control** { **aging** |**composition** | **history** | **length** } **enable**

6.1.10 password-control expired-user-login

Syntax

password-control expired-user-login delay *delay* **times** *times*

undo password-control expired-user-login

デフォルト

ユーザはパスワードの有効期限が終了したのち、30 日以内に 3 回ログインすることができます。すべてのログイン試行に失敗するか、30 日後にユーザがログイン試行を行うと、ユーザに新しいパスワードを設定するようプロンプトが表示されます。

View

System view

定義済みユーザロール

network-admin

パラメータ

delay *delay*: パスワードの有効期限が終了した後、ユーザがログインできる最大日時を設定します。設定範囲は 1〜90 日です。

times *times*: パスワードの有効期限が終了した後、ユーザがログインできる最大回数を設定します。設定範囲は 0〜10 です。パスワードの有効期限が終了した後、ユーザがシステムプロンプトで新しいパスワードを設定するには、値を 0 に設定します。

説明

password-control expired-user-login コマンドはパスワードの有効期限が終了した後、ユーザがログインできる最大日時と最大回数を設定します。

undo password-control expired-user-login コマンドはデフォルトに戻します。

このコマンドは、FTP 以外のログインユーザにのみ有効です。

FTP ユーザはパスワードの有効期限が終了した後、ログインすることができません。

例

パスワードの有効期限が終了した後、ユーザがログインできる最大日時を 60 日、最大回数を 5 回に設定します。

<AP> system-view

[AP] password-control expired-user-login delay 60 times 5

関連コマンド

display password-control

6.1.11 password-control history

Syntax

password-control history *max-record-number*

undo password-control history

デフォルト

4

View

System view

定義済みユーザロール

network-admin

パラメータ

max-record-number: 各ユーザのパスワード履歴の最大数を指定します。設定範囲は 2～15 です。

説明

password-control history コマンドは各ユーザのパスワード履歴の最大数を設定します。

undo password-control history コマンドはデフォルトに戻します。

パスワード履歴が最大数になったとき、後続のパスワード履歴はもっとも古いパスワードに上書きします。

システムは **undo password-control history enable** コマンドを実行した後、パスワードの記録を停止しますが、すでに記録されたパスワードを削除しません。

既存のパスワード履歴を削除する場合、以下のいずれかの方法を使用します。

- グローバルでパスワード管理機能を無効にするため、**undo password-control enable** コマンドを使用します。
- 手動でパスワードを削除するため、**reset password-control history-record** コマンドを使用します。

例

各ユーザのパスワード履歴の最大数を 10 に設定します。

<AP> system-view

[AP] password-control history 10

関連コマンド

- **display password-control**
- **password-control history enable**
- **reset password-control blacklist**

6.1.12 password-control length

Syntax

password-control length *length*

undo password-control length

デフォルト

グローバルの最小パスワード長は 10 文字です。

ユーザグループの最小パスワード長はグローバルの設定と同一です。ローカルユーザの最小パスワード長はローカルユーザが所属しているユーザグループの最小パスワード長と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

length: 最小パスワード長を指定します。設定範囲は 4～32 文字です。

説明

password-control length コマンドは最小パスワード長を設定します。

undo password-control length コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

最小パスワード長の設定は各 view に依存します。

- system view の最小パスワード長の設定はグローバルであり、すべてのユーザグループに適用します。
- user group view の最小パスワード長の設定はユーザグループのすべてのローカルユーザに適用します。
- local user view の最小パスワード長の設定はローカルユーザのみに適用します。

最小パスワード長の設定は小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view の最小パスワード長の設定を使用します。

- ローカルユーザに最小パスワード長が設定されていない場合、システムはローカルユーザが所属しているユーザグループの最小パスワード長の設定を使用します。
- ユーザグループに最小パスワード長が設定されていない場合、システムはグローバルの最小パスワード長の設定を使用します。

例

グローバルの最小パスワード長を 16 文字に設定します。

<AP> system-view

[AP] password-control length 16

ユーザグループ **test** の最小パスワード長を 16 文字に設定します。

[AP] user-group test

[AP-ugroup-test] password-control length 16

[AP-ugroup-test] quit

装置管理ユーザ **abc** の最小パスワード長を 16 文字に設定します。

[AP] local-user abc class manage

[AP-luser-manage-abc] password-control length 16

関連コマンド

- **display local-user**
- **display password-control**
- **display user-group**
- **password-control length enable**

6.1.13 password-control login idle-time

Syntax

password-control login idle-time *idle-time*

undo password-control login idle-time

デフォルト

90 日

View

System view

定義済みユーザロール

network-admin

パラメータ

idle-time: アカウントアイドルタイムの最大日数を指定します。設定範囲は 0～365 日です。0 はアカウントアイドルタイムの制限を行いません。

説明

password-control login idle-time コマンドはアカウントアイドルタイムの最大日数を設定します。

undo password-control login idle-time コマンドはデフォルトに戻します。

ユーザが最後にログインしてから指定した期間内にログインしない場合、ユーザアカウントは無効になります。

前回のログイン成功後にシステム時刻が変更されると、アカウントが無効になることがあります。無効なアカウントを使用してログインすることはできません。アカウントのアイドル時間制限を無効にするには、アイドル時間の値を 0 に設定します。

アカウントの最大アイドル時間はビューによって異なります。

- システムビューの時刻はグローバルな意味を持ち、すべてのユーザグループに適用されます。
- ユーザーグループビューの時刻は、ユーザグループ内のすべてのローカルユーザに適用されます。
- ローカルユーザビューの時刻は、ローカルユーザにのみ適用されます。

アプリケーションスコープが小さいアカウントの最大アイドル時間は優先度が高いです。システムは、ローカルユーザのローカルユーザビューでの最大アカウントアイドル時間を使用することを優先します

- ローカルユーザに最大アカウントアイドル時間が設定されていない場合、システムはローカルユーザが属するユーザグループの最大アカウントアイドル時間を使用します。
- ユーザグループに最大アカウントアイドル時間が設定されていない場合、システムはグローバル最大アカウントアイドル時間を使用します。

このコマンドは、装置管理ユーザだけが使用できます。

例

アカウントアイドルタイムの最大日数を 30 日に設定します。

<AP> system-view

[AP] password-control login idle-time 30

#ユーザグループ **test** の最大アカウントアイドル時間を 30 日に設定します。

[AP] user-group test

[AP -ugroup-test] password-control login idle-time 30

#装置管理ユーザ **abc** のアカウントの最大アイドル時間を 30 日に設定します

[AP] local-user abc class manage

[AP -luser-manage-abc] password-control login idle-time 30

関連コマンド

display password-control

6.1.14 password-control login-attempt

Syntax

password-control login-attempt *login-times* [**exceed** { **lock** | **lock-time** time [**autoincrement** max-lock-time] | **unlock** }]

undo password-control login-attempt

デフォルト

グローバルのログイン試行の設定は以下です。

- 連続してログインに失敗できる最大数は 3 です。
- 3 回ログインに失敗した後、ログインの試行を無効にする時間は 1 分です。

ユーザグループのログイン試行の設定はグローバルの設定と同一です。ローカルユーザのログイン試行の設定はローカルユーザが所属しているユーザグループのログイン試行の設定と同一です。

View

System view

User group view

Local user view

定義済みユーザロール

network-admin

パラメータ

login-times: 連続してログインに失敗できる最大数を指定します。設定範囲は 2～10 です。

exceed: ユーザが試行回数後にログインに失敗した後のアクションを指定します。

- **lock**: ユーザを永続的にロックします。
  - FTP、Web、または VTY ユーザの場合、ユーザアカウントとユーザの IP アドレスの両方がロックされます。このユーザアカウントを使用して、このロックされた IP アドレスからログインすることはできません。
  - コンソールユーザの場合、ユーザアカウントはロックされます。ユーザは、このユーザアカウントを使用してコンソールユーザ回線からログインすることはできません。
- **lock-time** *time*: 設定範囲は 1～360 分です。
  - ロックタイマの期限が切れると、FTP、Web、または VTY ユーザはこのユーザアカウントを使用して、IP アドレスから再度ログインできます。
  - ロックタイマの期限が切れると、コンソールユーザはこのユーザアカウントを使用して再度ログインできます。
- **autoincrement** *max-lock-time*: ロックタイマの期限が切れた後、アカウントが再度ログイン試行の最大回数に失敗するたびに、アカウントのロック期間をインクリメントできるようにします。*max-lock-time* 引数は、time 引数の値から 360 分の範囲で、最大ロック期間を表します。たとえば、time 引数が x で *max-lock-time* 引数が y の場合、アカウントが初めてログイン試行の最大回数に失敗したときに、アカウントが x 分間ロックされます。アカウントが n 回目のログイン試行の最大回数に失敗したとき、アカウントは n*x 分間ロックされます。n*x の積が y より大きい場合、アカウントは y 分間だけロックされ、その後のログイン失敗のロック期間は増加しません。

- **unlock**: ユーザアカウントをロックしません。
  - FTP、Web、または VTY ユーザは、このユーザアカウントを引き続き使用して、現在の IP アドレスからログインを試みることができます。
  - コンソールユーザは、このユーザアカウントを引き続き使用してログインを試行できます。No-

説明

password-control login-attempt コマンドはログイン試行の制限を設定します。ログイン最大試行回数と、ユーザが試行回数後にログインに失敗したときのアクションを設定できます。

undo password-control login-attempt コマンドはデフォルトに戻します。

ログイン試行の制限の設定は各 view に依存します。

- system view のログイン試行の制限の設定はグローバルであり、すべてのユーザグループに適用します。
- user group view のログイン試行の制限の設定はユーザグループのすべてのローカルユーザに適用します。
- local user view のログイン試行の制限の設定はローカルユーザのみに適用します。

ログイン試行の制限の設定は小さい範囲でのパスワードの設定が高い優先度を持ちます。システムはローカルユーザに local user view のログイン試行の制限の設定を使用します。

- ローカルユーザにログイン試行の制限が設定されていない場合、システムはローカルユーザが所属しているユーザグループのログイン試行の制限の設定を使用します。
- ユーザグループにログイン試行の制限が設定されていない場合、システムはグローバルのログイン試行の制限の設定を使用します。

FTP あるいは VTY ユーザが最大ログイン試行後にログインに失敗した場合、システムはユーザアカウントとユーザの IP アドレスをパスワード管理ブラックリストに追加します。

コンソールユーザも同様の操作でパスワード管理ブラックリストに追加します

アカウントは、ブラックリストに追加されたユーザのみロックされます。他のユーザはアカウントを使用することができます。ブラックリストに記載されているユーザは他のユーザアカウントを使用することができます。ロックされた IP アドレスのユーザに対してのみロックされます。ロック解除された IP アドレスのユーザはこのアカウントを使用でき、ロックされた IP アドレスのユーザは他のロック解除されたユーザアカウントを使用できます。

- ユーザのユーザアカウントが永久にロックされた場合、パスワード管理ブラックリストからアカウントを削除しない限り、ユーザはこのアカウントを使用することができません。ユーザアカウントを削除する場合、**reset password-control blacklist** コマンドを使用します。
- 一時的にロックされたユーザアカウントを使用する場合、以下のいずれかの処理を行うことができます。
  - ロックしているタイマが終了するまで待ちます。
  - パスワード管理ブラックリストからアカウントを削除します。

- ユーザアカウントとユーザがブラックリストに登録されているが、ロックされていない場合、ユーザは、このアカウントを使用してログインを行うことができます。ユーザがユーザアカウントを使用して装置に正常にログインしたとき、パスワード管理ブラックリストからアカウントとユーザの IP アドレスが削除されます。

🕮 **メモ：**

このアカウントは、ロックされた IP アドレスのユーザに対してのみロックされます。ロックされていない IP アドレスのユーザは引き続きこのアカウントを使用でき、ロックされた IP アドレスのユーザはロックされていない他のユーザアカウントを使用できます。

---

password-control login-attempt コマンドは、コマンドが設定されたのち、すぐに適用されます。パスワード管理ブラックリストにすでに存在するユーザも適用されます。

例

ユーザアカウントのログイン最大試行回数を 4 に設定し、ユーザが試行回数後にログインに失敗した後、ユーザアカウントを無効にします。

<AP> system-view

[AP] password-control login-attempt 4 exceed lock

装置にログインするユーザアカウント **test** を使用し、4 回間違ったパスワードを入力します。

パスワード管理ブラックリストを表示します。出力は、ブラックリストのユーザアカウントに存在し、アクションが **lock** であることを示します。

[AP] display password-control blacklist

```
Username: test
   IP: 192.168.44.1       Login failures: 4     Lock flag: lock

Blacklist items matched: 1.
```

192.168.44.1 のユーザが、このユーザアカウントを使用してログインできないことを確認します。

ユーザアカウントのログイン試行回数を 2 に設定し、ユーザが試行回数後にログインに失敗した後、3 分間、ユーザアカウントを無効にします。

<AP> system-view

[AP] password-control login-attempt 2 exceed lock-time 3

装置にログインするユーザアカウント **test** を使用し、2 回間違ったパスワードを入力します。

パスワード管理ブラックリストを表示します。出力は、ブラックリストのユーザアカウントに存在し、アクションが **lock** であることを示します。

[AP] display password-control blacklist

```
Username: test
   IP: 192.168.44.1       Login failures: 2     Lock flag: lock

Blacklist items matched: 1.
```

3 分後、ユーザアカウントがパスワード管理ブラックリストから削除され、192.168.44.1 のユーザが、このユーザアカウントを使用してログインできることを確認します。

関連コマンド

- **display local-user**
- **display password-control**
- **display password-control blacklist**
- **display user-group**
- **reset password-control blacklist**

6.1.15 password-control super aging

Syntax

password-control super aging *aging-time*

undo password-control super aging

デフォルト

90 日

View

System view

定義済みユーザロール

network-admin

パラメータ

aging-time: super パスワードの有効期限を指定します。設定範囲は 1～365 日です。

説明

password-control super aging コマンドは super パスワードの有効期限を設定します。

undo password-control super aging コマンドはデフォルトに戻します。

例

super パスワードの有効期限を 10 日に設定します。

<AP> system-view

[AP] password-control super aging 10

関連コマンド

- **display password-control**
- **password-control aging**

6.1.16 password-control super composition

Syntax

password-control super composition type-number *type-number* [**type-length** *type-length*]

undo password-control super composition

デフォルト

super パスワード構成ポリシーは少なくとも 2 種類の文字と各タイプに 1 文字以上を含む必要があります。

View

System view

定義済みユーザロール

network-admin

パラメータ

type-number *type-number*: super パスワードに含まれる文字タイプの最小数を指定します。設定範囲は 1～4 文字です。

type-length *type-length*: パスワードの各タイプの最小数を指定します。設定範囲は 1～63 です。

説明

password-control super composition コマンドは super パスワードの複雑性のポリシーを設定します。

undo password-control super composition コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

文字タイプの最小数と各タイプの最小文字数は super パスワードの最大長より小さくする必要があります。

例

super パスワードに少なくとも 4 種類の文字と各タイプに 5 文字以上を含むように指定します。

<AP> system-view

[AP] password-control super composition type-number 4 type-length 5

関連コマンド

- **display password-control**
- **password-control composition**

6.1.17 password-control super length

Syntax

password-control super length *length*

undo password-control super length

デフォルト

10 文字

View

System view

定義済みユーザロール

network-admin

パラメータ

length: super パスワードの最小パスワード長を指定します。設定範囲は 4～63 です。

説明

password-control super length コマンドは super パスワードの最小パスワード長を設定します。

undo password-control super length コマンドはデフォルトに戻します。

password-control enable コマンドを設定していなくても、本コマンドの設定が有効になります。

例

super パスワードの最小パスワード長を 16 文字に設定します。

<AP> system-view

[AP] password-control super length 16

関連コマンド

- **display password-control**
- **password-control length**

6.1.18 password-control update-interval

Syntax

password-control update-interval *interval*

undo password-control update-interval

デフォルト

24 時間

View

System view

定義済みユーザロール

network-admin

パラメータ

interval: パスワードアップデートの最小間隔を指定します。設定範囲は 0～168 時間です。0 はパスワードのアップデートを行わないことを示します。

説明

password-control update-interval コマンドはパスワードアップデートの最小間隔を設定します。パスワードアップデートの最小間隔はユーザがパスワードを変更できる最小間隔です。

undo password-control update-interval コマンドはデフォルトに戻します。

設定された最小間隔は、最初のログイン時またはパスワードの有効期限が切れた後にパスワードの変更を求められる装置管理ユーザでは有効ではありません。

例

パスワードアップデートの最小間隔を 36 時間に設定します。

<AP> system-view

[AP] password-control update-interval 36

関連コマンド

display password-control

6.1.19 reset password-control blacklist

Syntax

reset password-control blacklist [**user-name** *user-name*]

View

User view

定義済みユーザロール

network-admin

パラメータ

user-name *user-name*: パスワード管理ブラックリストから削除するユーザを指定します。設定範囲は 1～55 文字です。大文字、小文字を区別します。

説明

reset password-control blacklist コマンドはパスワード管理ブラックリストからユーザを削除します。

ログイン試行を超過したためにブラックリストに記録されたユーザが再度ログインできるようにするため、このコマンドを使用して、パスワード管理ブラックリストからユーザを削除します。

例

パスワード管理ブラックリストからユーザ **test** を削除します。

<AP> reset password-control blacklist user-name test

```
Are you sure to delete the specified user in blacklist? [Y/N]:
```

関連コマンド

display password-control blacklist

6.1.20 reset password-control history-record

Syntax

reset password-control history-record [**super** [**role** *role name*] | **user-name** *user-name* | **network-class** [**user-name** *user-name*]]

View

User view

定義済みユーザロール

network-admin

パラメータ

super: 指定された、あるいはすべての super パスワードの履歴の記録を削除します。

role *role name*: ユーザロールを指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。このオプションを指定しないと、すべての super パスワードの履歴の記録が削除されます。

network-class: ネットワークアクセスユーザの履歴パスワードレコードを削除します。このキーワードを指定しない場合、装置管理ユーザの履歴パスワードレコードが削除されます。

user-name *user-name*: パスワードレコードを削除するユーザのユーザ名を指定します。user-name 引数は、1 から 55 文字の文字列です。純粋なユーザ名を指定することも、純粋なユーザ名とそのドメイン名を純粋なユーザ名@ドメイン名の形式で指定することもできます。純粋なユーザ名では大文字と小文字が区別されます。ドメイン名では大文字と小文字が区別されません。ユーザ名を指定しない場合、このコマンドは、指定したユーザタイプの履歴パスワードレコードをすべて削除します。

説明

reset password-control history-record コマンドはパスワード履歴の記録を削除します。

パラメータを指定しない場合、すべてのローカルユーザのパスワード履歴の記録を削除します。

例

すべてのローカルユーザのパスワード履歴の記録を削除します。

<AP> reset password-control history-record

```
Are you sure to delete all local user's history records? [Y/N]:y
```

#すべてのネットワークアクセスユーザの履歴パスワードレコードを削除します。

<AP> reset password-control history-record network-class

```
Are you sure you want to delete all network access users' history records? [Y/N]:y
```

関連コマンド

password-control history

QX-W610 アクセスポイント

コマンドマニュアル

14.QoS

本マニュアルは以下に示す章で構成されています。

01-QoS
02-WLAN QoS

目次

このセクションのページは **14-x-x** です。

1 章 QoS 1-1
1.1 プライオリティマップ設定コマンド 1-1
1.1.1 display qos map-table 1-1
1.1.2 Import 1-3
1.1.3 qos map-table 1-4
1.2 プライオリティトラストモード設定コマンド 1-5
1.2.1 display qos trust interface 1-5
1.2.2 qos trust 1-7
1.3 ポートプライオリティ設定コマンド 1-8
1.3.1 qos priority 1-8

1章 QoS

1.1 プライオリティマップ設定コマンド

1.1.1 display qos map-table

Syntax

display qos map-table [**dot11e-lp | dot1p-lp | dscp-lp | lp-dot11e | lp-dot1p | lp-dscp**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

装置は表 1-1 に示すプライオリティマッピングを適用します。

表 1-1 プライオリティマッピング

プライオリティマッピング	説明
dot11e-lp	802.11e-localプライオリティマッピングです。
dot1p-lp	802.1p-localプライオリティマッピングです。
dscp-lp	DSCP-localプライオリティマッピングです。
lp-dot11e	Local-802.11eプライオリティマッピングです。
lp-dot1p	Local-802.1pプライオリティマッピングです。
lp-dscp	Local-DSCPプライオリティマッピングです。

説明

display qos map-table コマンドはプライオリティマッピングの設定を表示します。

プライオリティマップを指定しない場合、すべてのプライオリティマッピングの設定を表示します。

例

802.1p-local プライオリティマッピングの設定を表示します。

<AP> display qos map-table dot1p-lp

```
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define   DIRECTION: inbound
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

表 1-2 コマンド出力

フィールド	説明
MAP-TABLE NAME	プライオリティマッピングの名前です。
TYPE	プライオリティマッピングのタイプです。
IMPORT	プライオリティマッピングの入力値です。
EXPORT	プライオリティマッピングの出力値です。

1.1.2 Import

Syntax

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

デフォルト

デフォルトのプライオリティマッピングが使用されます。詳細は、オペレーションマニュアルのセクション 14 *QoS "QoS の設定"* を参照してください。

View

Priority map view

定義済みユーザロール

network-admin

パラメータ

import-value-list: 入力値のリストを指定します。

export-value: 出力値を指定します。

all: プライオリティマッピングのすべてのマッピングをデフォルトに戻します。

説明

import コマンドはプライオリティマッピングのマッピングを設定します。

undo import コマンドはプライオリティマッピングの指定した、あるいはすべてのマッピングをデフォルトに戻します。

例

802.1p-drop プライオリティマッピングを設定し、802.1p のプライオリティ 4 およびプライオリティ 5 を、ドロッププライオリティ 1 にマッピングします。

<AP> system-view

[AP] qos map-table dot1p-dp

[AP-maptbl-dot1p-dp] import 4 5 export 1

関連コマンド

display qos map-table

1.1.3 qos map-table

Syntax

qos map-table { **dot11e-lp | dot1p-lp | dscp-lp | lp-dot11e | lp-dot1p | lp-dscp** }

View

System view

定義済みユーザロール

network-admin

パラメータ

パラメータの説明は表 1-1 を参照してください。

説明

qos map-table コマンドは指定した priority map view に移行します。

例

802.1p-drop priority map view に移行します。

<AP> system-view

[AP] qos map-table dot1p-dp

[AP-maptbl-out-dot1p-dp]

関連コマンド

- **display qos map-table**
- **import**

1.2 プライオリティトラストモード設定コマンド

1.2.1 display qos trust interface

Syntax

display qos trust interface [*interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースのプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

説明

display qos trust interface コマンドはインタフェースのプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

例

GigabitEthernet 1/0/1 のプライオリティのトラステッドモードとポートプライオリティの情報を表示します。

<AP> display qos trust interface gigabitethernet 1/0/1

```
Interface: GigabitEthernet1/0/1
 Port priority information
  Port priority: 0
  Port dot1p priority: -
  Port dscp priority: -
  Port priority trust type: none
```

表 1-3 コマンド出力

フィールド	説明
Interface	インタフェースのタイプと番号です。
Direction	トラフィックポリシングが適用される方向です。

フィールド	説明
Port priority	インタフェースのポートプライオリティのセットです。
Rule	一致基準です。
CIR	CIRをkbps単位 (CIRが絶対値で指定されている場合) またはパーセンテージ単位 (CIRがパーセンテージで指定されている場合) で指定します。
CBS	CBSをバイト単位 (CBSが絶対値で指定されている場合) またはミリ秒単位 (CBSがミリ秒単位で指定されている場合) で指定します。CBSをミリ秒単位で指定した場合、実際のCBS値はcbs-time×実際のCIR値になります。
EBS	EBSをバイト単位 (EBSが絶対値で指定されている場合) またはミリ秒単位 (EBSがミリ秒単位で指定されている場合) で指定します。EBSをミリ秒単位で指定した場合、実際のEBS値はebs-time×実際のCIR値になります。
PIR	PIRをkbps単位 (PIRが絶対値で指定されている場合) またはパーセンテージ単位 (PIRがパーセンテージで指定されている場合) で指定します。
Green action	グリーンパケットに対して実行するアクションです。
Yellow action	イエローパケットに対して実行するアクションです。
Red action	レッドパケットに対して実行するアクションです。

1.2.2 qos trust

Syntax

qos trust { **dot1p** | **dscp** } [**override**]

undo qos trust

デフォルト

インタフェースはパケットのプライオリティを信用しません。802.1p プライオリティとしてポートプライオリティを使用します。

View

Interface view

定義済みユーザロール

network-admin

パラメータ

dot1p: プライオリティマッピングの受信パケットの 802.1p プライオリティを使用します。

dscp: プライオリティマッピングの受信パケットの DSCP を使用します。

override: 優先順位マッピングによって得られた優先順位を使用して、パケットで伝送された元の優先順位を上書きします。このキーワードはオプションです。デフォルトでは、この機能は無効になっています。

説明

qos trust コマンドはインタフェースのプライオリティトラステッドモードを設定します。

undo qos trust コマンドはデフォルトのプライオリティのトラステッドモードに戻します。

例

GigabitEthernet 1/0/1 のプライオリティトラステッドモードを 802.1p プライオリティに設定します。

<AP> system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] qos trust dot1p

関連コマンド

display qos trust interface

1.3 ポートプライオリティ設定コマンド

1.3.1 qos priority

Syntax

qos priority *priority-value*

undo qos priority

デフォルト

0

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

priority-value: ポートプライオリティの値を指定します。設定範囲は 0〜7 です。

説明

qos priority コマンドはインタフェースのポートプライオリティを変更します。

undo qos priority コマンドはデフォルトに戻します。

例

GigabitEthernet 1/0/1 のポートプライオリティを 2 に設定します。

<AP system-view

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] qos priority 2

関連コマンド

display qos trust interface

目次

このセクションのページは **14-x-x** です。

2 章 WLAN QoS 2-1
2.1 WLAN QoS 設定コマンド 2-1
2.1.1 atf 2-1
2.1.2 bandwidth-guarantee 2-2
2.1.3 bandwidth-guarantee service-template 2-3
2.1.4 client-rate-limit 2-4
2.1.5 display wlan wmm 2-5
2.1.6 edca client (ac-be | ac-bk) 2-9
2.1.7 edca client (ac-vi | ac-vo) 2-10
2.1.8 edca radio 2-12
2.1.9 qos priority 2-14
2.1.10 qos trust 2-15
2.1.11 reset wlan wmm 2-16
2.1.12 wlan client-rate-limit 2-17
2.1.13 wlan max-bandwidth 2-18
2.1.14 wmm 2-19

2章 WLAN QoS

2.1 WLAN QoS設定コマンド

2.1.1 atf

Syntax

atf { **disable** | **enable** }

undo atf

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

説明

atf enable コマンドは Air Time Fairness 機能を有効にします。

atf disable コマンドは Air Time Fairness 機能を無効にします。

undo atf コマンドはデフォルトに戻します。

Air Time Fairness は、すべてのクライアントが AP のカバレッジエリア内の通信時間に均等にアクセスできるようにします。この機能を使用すると、高速クライアントがワイヤレスリソースを使用する機会が増えます。これにより、ネットワーク全体の転送効率が向上します。

この機能を有効にすると、AP からクライアント方向の通信のネットワーク転送効率の向上が期待されますが、低速クライアントの転送効率が低下する可能性があります。

この機能を設定する場合は、アクセスクライアントの数と高速クライアントの転送効率を考慮してください。

例

AP ap1 の Radio 1 で Air Time Fairness 機能を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] atf enable

2.1.2 bandwidth-guarantee

Syntax

bandwidth-guarantee { **disable** | **enable** }

undo bandwidth-guarantee

デフォルト

無効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: 帯域保証を無効にします。

enable: 帯域保証を有効にします。

説明

bandwidth-guarantee enable コマンドは帯域保証を有効にします。

bandwidth-guarantee disable コマンドは帯域保証を無効にします。

undo bandwidth-guarantee コマンドはデフォルトに戻します。

このコマンドを使用すると、ネットワークが混雑しているときに、同じ無線に関連付けられたクライアントが保証帯域幅を取得できるようになります。保証帯域幅を設定するには、**bandwidth-guarantee service-template** コマンドを使用します。

例

帯域保証を有効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] service-template 1

[AP-WLAN-Radio1/0/1] bandwidth-guarantee enable

関連コマンド

bandwidth-guarantee service-template

2.1.3 bandwidth-guarantee service-template

Syntax

bandwidth-guarantee service-template *service-template-name* **percent** *percent*

undo bandwidth-guarantee { **all** | **service-template** *service-template-name* }

デフォルト

設定なし

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

service-template *service-template-name*: サービステンプレートを名前で指定します。大文字と小文字を区別しません。設定範囲は 1～63 文字です。指定したサービステンプレートが無線に紐づけられていることを確認してください。

percent *percent*: 総帯域幅に対する保証帯域幅の割合を指定します。*percent* 引数の値の範囲は 1～100 です。合計帯域幅は、無線の最大帯域幅を示します。保証帯域幅は、サービステンプレートに対応する BSS の最小帯域幅を示します。

all: すべてのサービステンプレートを指定します。

説明

bandwidth-guarantee service-template コマンドは指定されたサービステンプレートの保証帯域幅の割合を設定します。

undo bandwidth-guarantee service-template コマンドは指定されたサービステンプレートの保証帯域幅設定をキャンセルします。

このコマンドを有効にするには、帯域保証機能が有効になっていることを確認してください。

同じ無線に紐づけられているすべてのサービステンプレートで、保証帯域幅の合計が 100%を超えることはできません。

例

サービステンプレート 1 の保証帯域幅の割合を 30%に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] service-template 1

[AP-WLAN-Radio1/0/1] bandwidth-guarantee enable

[AP-WLAN-Radio1/0/1] bandwidth-guarantee service-template 1 percent 30

関連コマンド

- **bandwidth-guarantee**
- **wlan max-bandwidth**

2.1.4 client-rate-limit

Syntax

client-rate-limit { **inbound** | **outbound** } **mode** { **dynamic cir** *cir* [**min** *min-cir*] [**max** *max-cir*] | **static cir** *cir* } [**cbs** *cbs*]

undo client-rate-limit { **inbound** | **outbound** }

デフォルト

設定なし

View

Service template view

定義済みユーザロール

network-admin

パラメータ

inbound: 受信トラフィックのレートを制限します。

outbound: 送信トラフィックのレートを制限します。

dynamic: 動的レート制限モードを指定します。このモードでは、各クライアントの最大レートは、合計最大レートをクライアント数で割った値になります。

cir *cir*: CIR を Kbps で指定します。cir 引数の値は 16～1700000 の範囲です。このオプションは、静的レート制限モードの場合は各クライアントの最大レートを設定し、動的レート制限モードの場合はすべてのクライアントの最大レートを設定します。

min *min-cir*: クライアントの最小 CIR を 16 から 1700000Kbps の範囲で指定します。

max *max-cir*: クライアントの最大 CIR を 16 から 1700000Kbps の範囲で指定します。

static: 静的レート制限モードを指定します。各クライアントの最大レートは固定です。

cbs *cbs*: CBS をバイト単位で指定します。cbs 引数の値の範囲は 1～268435456 です。このオプションを指定しない場合、CBS の値は CIR の値から自動的に計算されます。

説明

client-rate-limit コマンドはサービステンプレートベースのクライアントレート制限を設定します。

undo client-rate-limit コマンドはデフォルトに戻します。

このコマンドを複数回繰り返して、受信トラフィックと送信トラフィックの両方のレートを制限できます。

例

サービステンプレート 1 のレート制限を設定します。各クライアントの受信トラフィックに対して CIR を 567 Kbps に設定します。

<AP> system-view

[AP] wlan service-template 1

[AP-wlan-st-1] client-rate-limit enable

[AP-wlan-st-1] client-rate-limit inbound mode static cir 567

関連コマンド

client-rate-limit enable

2.1.5 display wlan wmm

Syntax

display wlan wmm { **client** [**interface wlan-radio** *interface-number* | **mac-address** *mac-address*] | **radio** [**interface wlan-radio** *interface-number*] }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

client: クライアントの WMM の統計情報を表示します。**interface wlan-radio** *interface-number* または **mac-address** *mac-address* オプションを指定せずにこのキーワードを使用すると、このコマンドはすべてのクライアントの WMM 統計情報を表示します。

radio: 無線の WMM の統計情報を表示します。**interface wlan-radio** *interface-number* を指定せずにこのキーワードを使用すると、このコマンドはすべての無線の WMM 統計情報を表示します。

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H 形式で指定します。

interface wlan-radio *interface-number*: 無線インタフェースを番号で指定します。

説明

display wlan wmm コマンドは WMM の統計情報を表示します。

例

すべての無線の WMM 統計情報を表示します。

<AP> display wlan wmm radio

```
Radio : 1
Client EDCA updates : 0
QoS mode  : WMM
WMM status : Enabled
Radio max AIFSN    : 15              Radio max ECWmin : 10
Radio max TXOPLimit : 32767           Radio max ECWmax : 10

Radio : 2
Client EDCA updates : 0
QoS mode  : WMM
WMM status: Disabled
Radio max AIFSN    : 15              Radio max ECWmin : 10
Radio max TXOPLimit : 32767           Radio max ECWmax : 10
```

表 2-1 コマンド出力

フィールド	説明
Client EDCA updates	クライアントのEDCAパラメータが更新された回数です。
QoS mode	WMM このフィールドがN/Aと表示する場合、QoSモードは利用できません。
WMM status	• Enable • Disable
Radio max AIFSN	無線がサポートする最大AIFSNです。
Radio max ECWmin	無線がサポートする最大ECWminです。
Radio max TXOPLimit	無線がサポートする最大TXOPLimitです。
Radio max ECWmax	無線がサポートする最大ECWmaxです。
Total request medium time	AC-VOおよびAC-VIキューの合計要求メディア時間 (マイクロ秒)です 。

#すべてのクライアントの WMM 統計情報を表示します。

<AP> display wlan wmm client

```
MAC address : 00ff-e23c-0001          SSID : service
QoS mode : WMM
APSD information :
  Max SP length : 7
  L: Legacy    T: Trigger      D: Delivery
  AC           AC-BK   AC-BE   AC-VI    AC-VO
  Assoc State   T|D     L      T|D      T|D
Statistics information :
  Uplink packets     : 0          Downlink packets  : 0
  Uplink bytes       : 0          Downlink bytes    : 0
  Downgrade packets      : 0          Discarded packets      : 0
  Downgrade bytes        : 0          Discarded bytes        : 0
TS information:
  AC                 : AC-VO       User priority            : 7
  TID                : 1           Direction                : Bidirectional
  PSB                : 0           Surplus bandwidth allowance : 1.0000
  Medium time (μs)     : 39          MSDU size (bytes)          : 1500
  Mean data rate (Kbps) : 10.000       Minimum PHY rate (Mbps)     : 11.000
  TS creation time     : 0h:0m:5s
  TS updating time     : 0h:0m:5s
  Uplink TS packets    : 0          Downlink TS packets        : 0
  Uplink TS bytes      : 0          Downlink TS bytes          : 0
```

表 2-2 コマンド出力

フィールド	説明
QoS mode	• **WMM** • **N/A**
Max SP length	最大サービス期間(SP)の長さです。
AC	• AC-VO • AC-VI • AC-BE • AC-BK
Assoc state	ACキューのAPSD属性です。 • **T**－ACキューがtrigger-enabledです。 • **D**－ACキューがdelivery-enabledです。 • **T	D**－ACキューは、trigger-enabledとdelivery-enabledの両方です。 • **L**－ACはレガシー属性のものです。

フィールド	説明
User priority	有線ネットワークからのパケットのユーザ優先度です。
TID	トラフィック識別子です。範囲は0～15です。
Direction	トラフィック方向です。 ● Uplink ● Downlink ● Bidirectional
PSB	省電力動作です。 ● **1**－U-APSD省電力モードです。 ● **0**－従来の省電力モードです。
Surplus bandwidth allowance	余剰帯域幅のパーセンテージです。
Medium time	許容される中間時間(マイクロ秒)です。
MSDU size	平均MSDUサイズ(バイト)です。
Mean data rate	平均データ転送速度(Kbps)です。
Minimum PHY rate	最小物理伝送速度(Mbps)です。

関連コマンド

reset wlan wmm

2.1.6 edca client (ac-be | ac-bk)

Syntax

edca client { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo edca client { **ac-be** | **ac-bk** }

デフォルト

クライアントの AC-BE キューと AC-BK キューのデフォルトの EDCA パラメータ値を表 2-3 に示します。

表 2-3 クライアントの AC-BE キューと AC-BK キューのデフォルト EDCA パラメータ値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	10	0

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を指数形式で 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）を指数形式で 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

txoplimit *txoplimit-value*: TXOP Limit（transmission opportunity limit）値を 0～65535（32 マイクロ秒単位）の範囲で指定します。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットしか送信できません。

説明

wmm edca client コマンドはクライアントの AC-BE キューまたは AC-BK キューの EDCA パラメータを設定します。

undo wmm edca client コマンドはデフォルトに戻します。

すべてのクライアントが 802.11b クライアントである場合、AC-BE キューと AC-BK キューのそれぞれに対して TXOP Limit 値を 0 に設定することを推奨します。

802.11b と 802.11g の両方のクライアントが WLAN に存在する場合、AC-BK と AC-BE のそれぞれのキューにデフォルトの TXOPLimit 値を使用することを推奨します。

例

AC-BE キューの AIFSN を 5 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] edca client ac-be aifsn 5

2.1.7 edca client (ac-vi | ac-vo)

Syntax

edca client { **ac-vi** | **ac-vo** } { **aifsn** *aifsn-value* | **cac** { **disable** | **enable** } | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo edca client { **ac-vi** | **ac-vo** }

デフォルト

クライアントの AC-VI キューと AC-VO キューのデフォルトの EDCA パラメータ値を表 2-4 に示します。

表 2-4 クライアントの AC-BE キューと AC-BK キューのデフォルト EDCA パラメータ値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-VI	2	3	4	94
AC-VO	2	2	3	47

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

aifsn *aifsn-value*: AIFSN（arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

cac: CAC を指定します。AC-VO および AC-VI キューは CAC をサポートします。CAC はデフォルトで無効になっています。

disable: CAC を無効にします。

enable: CAC を有効にします。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）を指数形式で 0～15 の範囲で指定します。

ecwmax *ecwmax-value*: ECWmax （the exponent form of CWmax）を指数形式で 0～15 の範囲で指定します。ECWmax の値は ECWmin の値より小さくすることはできません。

txoplimit *txoplimit-value*: TXOP Limit（transmission opportunity limit）値を 0～65535（32 マイクロ秒単位）の範囲で指定します。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットしか送信できません。

説明

wmm edca client コマンドはクライアントの AC-VI または AC-VO キューの EDCA パラメータを設定します。

undo wmm edca client コマンドはデフォルトに戻します。

すべてのクライアントが 802.11b クライアントである場合、AC-VI および AC-VO キューの TXOPLimit 値をそれぞれ 188 と 102 に設定することを推奨します。

802.11b と 802.11g のそれぞれのクライアントが WLAN に存在する場合、AC-VI と AC-VO のそれぞれのキューにデフォルトの TXOPLimit 値を使用することを推奨します。

例

AC-VO キューの AIFSN を 3 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] edca client ac-vo aifsn 3

2.1.8 edca radio

Syntax

edca radio { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** } { **ack-policy** { **noack** | **normalack** } | **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **noack** | **txoplimit** *txoplimit-value* } *

undo edca radio { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** }

デフォルト

デフォルトの EDCA パラメータ値を表 2-5 に示します。

表 2-5 EDCA パラメータのデフォルト値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	6	0
AC-VI	1	3	4	94
AC-VO	1	2	3	47

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

ac-be: AC-BE（ベストエフォート型トラフィック）キューを指定します。

ac-bk: AC-BK（バックグラウンドトラフィック）キューを指定します。

ac-vi: AC-VI（ビデオトラフィック）キューを指定します。

ac-vo: AC-VO（音声トラフィック）キューを指定します。

ack-policy: AC キューの ACK ポリシーを指定します。

noack: No ACK ポリシー（デフォルト）を指定します。

normalack: Normal ACK ポリシーを指定します。

aifsn *aifsn-value*: AIFSN（Arbitration inter-frame spacing number）を 1～15 の範囲で指定します。

ecwmin *ecwmin-value*: ECWmin（the exponent form of CWmin）の指数形式を指定します。*ecwmin-value* 引数の値の範囲は 0～10 です。

ecwmax *ecwmax-value*: ECWmax（the exponent form of CWmax）の指数形式を指定します。*ecwmax-value* 引数の値の範囲は 0～10 です。ECWmax の値は ECWmin の値より小さくすることはできません。

txopimit *txoplimit-value*: Transmission opportunity limit（TXOP Limit）の値を 32 マイクロ秒単位で指定します。*txoplimit-value* 引数の値の範囲は 0～32767 です。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットのみを送信できます。

説明

edca radio コマンドは EDCA パラメータを設定します。

undo edca radio コマンドはデフォルトに戻します。

802.11b 無線の場合、AC-BK、AC-BE、AC-VI、AC-VO キューの TXOP 制限値をそれぞれ 0、0、188、102 に設定することを推奨します。

例

無線 2 の radio view で、AC-VO キューの AIFSN を 2 に設定します。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] edca radio ac-vo aifsn 2

2.1.9 qos priority

Syntax

qos priotity *priority*

undo qos priotity

デフォルト

0

View

Service template view

定義済みユーザロール

network-admin

パラメータ

priority: ポートプライオリティを 0～7 の範囲で指定します。値が大きいほど優先度が高くなります。

説明

qos priority コマンドはポートプライオリティを設定します。

undo qos priority コマンドはデフォルトに戻します。

ポートトラステッドモードが有効な場合、AP はポートプライオリティをサービステンプレートのすべてのパケットに割り当てます。

パケットトラステッドモードが有効な場合、このコマンドは有効になりません。

例

サービステンプレート 1 のポートプライオリティを 2 に設定します。

<AP> system

[AP] wlan service-template 1

[AP-wlan-st-1] qos priority 2

関連コマンド

qos trust

2.1.10 qos trust

Syntax

qos trust { **dot11e** | **dscp** }

undo qos trust

デフォルト

ポートプライオリティを使用する

View

Service template view

定義済みユーザロール

network-admin

パラメータ

dot11e: 優先度マッピングのためにパケット内で運ばれる 802.11e 優先度を使用します。

dscp: 優先度マッピングのためにパケット内で運ばれる DSCP 優先度を使用します。

説明

qos trust コマンドはパケットトラステッドモードを有効にします。

undo qos trust コマンドはデフォルトに戻します。

この機能はアップリンクパケットでのみ有効です。

例

サービステンプレート 1 のパケットトラストモードを有効にします。

<AP> system

[AP] wlan service-template 1

[AP-wlan-st-1] qos trust dot11e

関連コマンド

qos priority

2.1.11 reset wlan wmm

Syntax

reset wlan wmm { **client** [**interface wlan-radio** *interface-number* | **mac-address** *mac-address*] | **radio** [**interface wlan-radio** *interface-number*] }

View

ユーザ view

定義済みユーザロール

network-admin

パラメータ

client: クライアントの WMM 統計情報を削除します。**interface wlan-radio** *interface-number* または **mac-address** *mac-address* オプションを指定せずにこのキーワードを使用すると、このコマンドはすべてのクライアントの WMM 統計情報をクリアします。

radio: 無線の WMM 統計情報を削除します。**interface wlan-radio** *interface-numbe*r オプションを指定せずにこのキーワードを使用すると、このコマンドはすべての無線の WMM 統計情報をクリアします。

mac-address *mac-address*: クライアントの MAC アドレスを H-H-H 形式で指定します。

interface wlan-radio *interface-number*: 無線インタフェースを番号で指定します。

説明

reset wlan wmm コマンドは WMM 統計情報を削除します。

例

すべての無線の WMM 統計情報を削除します。

<AP> reset wlan wmm radio all

関連コマンド

display wlan wmm

2.1.12 wlan client-rate-limit

Syntax

wlan client-rate-limit { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | | **dot11gax** | **dot11gn** } { **inbound** | **outbound** } **cir** *cir* [**cbs** *cbs*]

undo wlan client-rate-limit [{ **dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | **dot11gax** | **dot11gn** } [**inbound** | **outbound**]]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a クライアントを指定します。

dot11ac: 802.11ac クライアントを指定します。

dot11an: 802.11an クライアントを指定します。

dot11ax: 802.11ax クライアントを指定します。

dot11b: 802.11b クライアントを指定します。

dot11g: 802.11g クライアントを指定します。

dot11gn: 802.11gn クライアントを指定します。

dot11gax: 802.11gax クライアントを指定します。

inbound: 受信トラフィックのレートを制限します。

outbound: 送信トラフィックのレートを制限します。

cir *cir*: 各クライアントの CIR を Kbps 単位で指定します。*cir* 引き数の値は 1～2097152 の範囲です。

cbs *cbs*: 各クライアントの CBS をバイト単位で指定します。*cbs* 引数の値は 1～268435456 の範囲です。このオプションを指定しない場合、CBS の値は CIR の値から自動的に計算されます。

説明

wlan client-rate-limit コマンドはクライアントタイプベースのクライアントレート制限を設定します。

undo wlan client-rate-limit コマンドは設定を削除します。

クライアントレート制限のために、異なるレート制限方式とレート制限モードを設定することができ、すべての設定が有効になります。これらの設定間のうちレート制限の最小値が各クライアントに適用されます。

例

802.11an クライアントの受信トラフィックのレート制限を 20480 Kbps に設定します。

<AP> system-view

[AP] wlan client-rate-limit dot11an inbound cir 20480

2.1.13 wlan max-bandwidth

Syntax

wlan max-bandwidth { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | **dot11gn** | **dot11gax** } *bandwidth*

undo wlan max-bandwidth [**dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | **dot11gn** | **dot11gax**]

デフォルト

次の最大帯域幅設定が適用されます。

- dot11a と dot11g に対して 30000 Kbps
- dot11an と dot11gn と dot11gax に対して 250000 Kbps
- dot11ac と dot11ax では 500000 Kbps
- dot11b では 7000 Kbps

View

System view

定義済みユーザロール

network-admin

パラメータ

dot11a: 802.11a 無線モードを指定します。

dot11ac: 802.11ac 無線モードを指定します。

dot11an: 802.11an 無線モードを指定します。

dot11ax: 802.11ax 無線モードを指定します。

dot11b: 802.11b 無線モードを指定します。

dot11g: 802.11g 無線モードを指定します。

dot11gn: 802.11gn 無線モードを指定します。

dot11gax: 802.11gax 無線モードを指定します。

bandwidth: 最大帯域幅を Kbps 単位で指定します。値の範囲は、無線の種類によって次のように変化します。

- dot11a と dot11g は 16～30000 です。
- dot11an と dot11gn と dot11gax は 16～250000 です。
- dot11ac と dot11ax は 16～500000 です。
- dot11b は 16～7000 です。

説明

wlan max-bandwidth コマンドは無線タイプごとの最大帯域幅を設定します。

undo wlan max-bandwidth コマンドは指定した無線タイプのデフォルト設定またはすべての無線タイプのデフォルトに戻します。

最大帯域幅は、保証された帯域幅を計算するために使用されます。

例

802.11ac の最大帯域幅を 2000 Kbps に設定します。

<AP> system-view

[AP] wlan max-bandwidth dot11ac 2000

2.1.14 wmm

Syntax

wmm { **disable** | **enable** }

undo wmm

デフォルト

有効

View

Radio interface view

定義済みユーザロール

network-admin

パラメータ

disable: WMM を無効にします。

enable: WMM を有効にします。

説明

wmm enable コマンドは WMM を有効にします。

wmm disable コマンドは WMM を無効します。

undo wmm コマンドはデフォルトに戻します。

すべての 802.11 n、802.11 ac、および 802.11 ax クライアントは WLAN QoS をサポートしている必要があります。 802.11n、802.11ac、802.11ax クライアントが関連する AP と通信するために、無線が 802.11an、802.11gn、802.11ac、802.11ax モードで動作しているときに WMM を有効にしてください。

例

WMM を無効にします。

<AP> system-view

[AP] interface wlan-radio 1/0/1

[AP-WLAN-Radio1/0/1] wmm disable

QX-W610 アクセスポイント

コマンドマニュアル

15. ネットワーク管理とモニタ

本マニュアルは以下に示す章で構成されています。

01-システムの保守とデバッグ

02-NQA

03-SNMP

04-NETCONF

05-プロセスモニタリングとメンテナンス

06-NetMeister

目次

このセクションのページは **15-x-x** です。

1 章 システムの保守とデバッグ 1-1
1.1 システムの保守とデバッグ設定コマンド 1-1
1.1.1 debugging 1-1
1.1.2 display debugging 1-3
1.1.3 ping 1-4
1.1.4 tracert 1-8

1章 システムの保守とデバッグ

1.1 システムの保守とデバッグ設定コマンド

1.1.1 debugging

Syntax

debugging *module-name* [*option*]

undo debugging { **all** | *module-name* [*option*] }

デフォルト

無効

View

User view

定義済みユーザロール

network-admin

パラメータ

module-name: arp、device のようなモジュール名を指定します。現在のモジュール名を表示する場合、**debugging ?**コマンドを使用します。

option: モジュールのデバッグオプションを指定します。オプションの番号と内容はモジュールによって異なります。サポートされるオプションを表示する場合、**debugging** *module-name* **?**コマンドを使用します。

all: すべてのデバッグを指定します。

説明

debugging コマンドは指定したモジュールのデバッグを有効にします。

undo debugging コマンドは指定したモジュールあるいはすべてのモジュールのデバッグを無効にします。

⚠ **注意:**

過剰なデバッグメッセージが出力されると、CPU 使用率が増加し、システムパフォーマンスが低下します。システムパフォーマンスを保証するには、例外的な状態にあるモジュールに対してのみデバッグを有効にします。

システムは生成されたデバッグメッセージを Information Center に送信します。ログの出力設定にもとづいて適切な宛先に送信します。Information Center の詳細はオペレーションマニュアルのセクション 2 *システム管理 "Information Center"* を参照してください。

例

装置管理モジュールのデバッグを有効にします。

<AP> debugging dev

関連コマンド

display debugging

1.1.2 display debugging

Syntax

display debugging [*module-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

module-name: モジュール名を指定します。現在のモジュール名を表示する場合、**debugging ?**コマンドを使用します。指定しない場合、すべてのモジュールにおいて有効になっているデバッグ機能を表示します。

説明

display debugging コマンドは有効になっているデバッグ機能を表示します。

例

有効になっているすべてのデバッグ機能を表示します。

<AP> display debugging

```
DEV debugging switch is on
```

関連コマンド

debugging

1.1.3 ping

Syntax

ping [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v**] * *host*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

ip: 宛先ホストの名前が **i**、**ip**、**ipv**、**ipv6**、**l**、**ls**、**lsp** であるとき、宛先ホスト名と **ping** コマンドのパラメータを区別します。たとえば、宛先ホスト名が ip である場合、**ping** *ip* の代わりに **ping ip** *ip* の形式を使用する必要があります。

-a *source-ip*: ICMP エコー要求の送信元 IP アドレスとして装置の IP アドレスを指定します。指定しない場合、ICMP エコー要求の送信元 IP アドレスは送信インタフェースのプライマリ IP アドレスです。

-c *count*: 宛先に送信する ICMP エコー要求の数を指定します。設定範囲は 1～4294967295 です。デフォルトは 5 です。

-f: IP ヘッダの DF（do-not-fragment）ビットを設定します。

-h *ttl*: ICMP エコー要求の TTL を指定します。設定範囲は 1～255 です。デフォルトは 255 です。

-i *interface-type interface-number*: ICMP エコー要求の送信元インタフェースを指定します。指定しない場合、ICMP エコー要求の送信元インタフェースとしてルートの出力インタフェースに一致するプライマリ IP アドレスを使用します。

-m *interval*: ICMP エコー要求を送信する間隔を指定します。設定範囲は 1～65535 ミリ秒です。デフォルトは 200 ミリ秒です。

-n: *host* のドメイン名解決を無効にします。*host* は宛先のホスト名を示します。指定しない場合、装置はホストをアドレスに変換します。

-p *pad*: ICMP エコー要求のパディングフィールドの値を指定します。設定範囲は 16 進数、1～8 ビットで 0～ffffffff です。指定した値が 8 ビット未満の場合、上位ビットに 0 が追加され 8 ビットに拡張されます。たとえば、*pad* が 0x2f に設定されている場合、装置が要求するパケット長にするために、パケットは 0x0000002f のパディングフィールドで埋められます。パディングの値のデフォルトは 0x01 で始まり 0xff までです。必要があれば、再度繰り返します。たとえば 0x010203…feff01….です。

-q: 統計情報の概要を表示します。指定しない場合、ping のすべての統計情報を表示します。

-r: パスの ICMP エコー要求の Hop アドレス（9 まで）を記録します。指定しない場合、パスの ICMP エコー要求の Hop アドレス（9 まで）を記録しません。

-s *packet-size*: IP パケットヘッダと ICMP パケットヘッダを除く ICMP エコー要求の長さを指定します。設定範囲は 20～8100 バイトです。デフォルトは 56 バイトです。

-t *timeout*: ICMP エコー応答のタイムアウト時間を指定します。設定範囲は 0～65535 ミリ秒です。デフォルトは 2000 ミリ秒です。タイムアウト時間内に送信元が ICMP エコー応答を受信しない場合、ICMP エコー応答がタイムアウトしたと認識します。

-tos *tos*: ICMP エコー要求の ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

-v: ICMP 以外のエコー応答を表示します。指定しない場合、システムは ICMP 以外のエコー応答を表示しません。

host: 宛先の IP アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

説明

ping コマンドは IP ネットワーク内の宛先装置が到達可能かどうかを検証し、関連する統計情報を表示します。

ping コマンドで宛先ホストの名前を使用する場合、先に装置の DNS の設定を行う必要があります。そうでなければ **ping** コマンドは失敗します。

ping コマンドを実行中、**Ctrl+C** を押下することで中止することができます。

例

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。

<AP> ping 1.1.2.2

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。統計情報のみを表示します。

<AP> ping -q 1.1.2.2

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
```

```
--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.962/2.196/2.665/0.244 ms
```

IP アドレス 1.1.2.2 の装置が到達可能かどうかを検証します。パスの ICMP パケットが通過する Hop アドレスを表示します。

<AP> ping -r 1.1.2.2

```
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms
RR:     1.1.2.1
        1.1.2.2
        1.1.1.2
        1.1.1.1
56 bytes from 1.1.2.2: icmp_seq=1 ttl=254 time=4.834 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=2 ttl=254 time=4.770 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=3 ttl=254 time=4.812 ms  (same route)
56 bytes from 1.1.2.2: icmp_seq=4 ttl=254 time=4.704 ms  (same route)

--- Ping statistics for 1.1.2.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms
```

出力は以下のことを示します。

- 宛先装置へ到達可能です。
- ルートは 1.1.1.1 <-> {1.1.1.2; 1.1.2.1} <-> 1.1.2.2 です。

表 1-1 コマンド出力

フィールド	説明
Ping 1.1.2.2 (1.1.2.2): 56 data bytes, press CTRL_C to break	IPアドレス1.1.2.2の装置に到達可能かどうかを検証します。各ICMPエコー要求のパケット長は56バイトです。pingを中止する場合、**Ctrl+C**を押下します。
56 bytes from 1.1.2.2: icmp_seq=0 ttl=254 time=4.685 ms	IPアドレス1.1.2.2の装置からICMPエコー応答を受信しました。タイムアウト時間内にエコー応答がない場合、表示されません。 • **bytes**—ICMPエコー応答のバイト数です。 • **icmp_seq**—セグメントが紛失、順番が異常、繰り返ししているかどうかを確認するために使用されるパケットシーケンスです。 • **ttl**—ICMPエコー応答のTTLです。 • **time**—応答時間です。
RR:	ICMPエコー要求を通過したルータです。遠いところから順番に表示されます。宛先にもっとも近いルータが最初に表示されます。

フィールド	説明
--- Ping statistics for 1.1.2.2 ---	pingで送受信した統計情報です。
5 packet(s) transmitted	送信したICMPエコー要求の数です。
5 packet(s) received	受信したICMPエコー要求の数です。
0.0% packet loss	送信したパケットに対して応答がないパケットの割合です。
round-trip min/avg/max/std-dev = 4.685/4.761/4.834/0.058 ms	最小/平均/最大/標準の応答時間です。単位はミリ秒です。

1.1.4 tracert

Syntax

tracert [**-a** *source-ip* | **-f** *first-ttl* | **-i** *interface-type interface-number* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-s** *packet-size* | **-t** *tos* | **-w** *timeout*] * *host*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

-a *source-ip*: プローブパケットの送信元 IP アドレスとして装置の IP アドレスを指定します。指定しない場合、プローブパケットの送信元 IP アドレスは送信インタフェースのプライマリ IP アドレスです。

-f *first-ttl*: 宛先に送信された最初のパケットの TTL を指定します。設定範囲は 1～255 です。デフォルトは 1 です。この値は *max-ttl* 以下の値でなければなりません。

-i *interface-type interface-number*: プローブパケットの送信元インタフェースを指定します。このオプションを指定しない場合、システムは一致するルートのルーティングテーブルまたは転送テーブルを検索し、そのルートの出力インタフェースをプローブパケットの送信元インタフェースとして使用します。

-m *max-ttl*: プローブパケットで許可される最大 Hop 数を指定します。設定範囲は 1～255 です。デフォルトは 30 です。この値は *first-ttl* 以上の値でなければなりません。

-p *port*: 宛先の無効の UDP ポートを指定します。設定範囲は 1～65535 です。デフォルトは 33434 です。

-q *packet-number*: ホップごとに送信されるプローブパケット数を指定します。設定範囲は 1～65535 です。デフォルトは 3 です。

-s *packet-size*: プローブパケットのペイロード長をバイト単位で指定します。packet-size 引数の値の範囲は 12～9600 です。デフォルトの設定は 12 バイトです。

-t *tos*: プローブパケットの ToS 値を指定します。値の範囲は 0～255 で、デフォルトは 0 です。

-w *timeout*: プローブパケットの応答パケットのタイムアウト時間を指定します。設定範囲は 1～65535 ミリ秒です。デフォルトは 5000 ミリ秒です。

host: 宛先の IP アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。

説明

tracert コマンドはパケットが送信元から宛先に向かう間に通過するルートを追跡します。

ping コマンドでネットワークの故障を識別したのち、**tracert** コマンドで故障したノードの位置を見つけることができます。

tracert コマンドの出力情報には、パケットが送信元から宛先に向かう間に通過するすべてのルートの IP アドレスが含まれます。ICMP エラーメッセージで装置が応答しない場合、アスタリスク（*.*.*）が表示されます。（宛先が到達不能あるいは ICMP タイムアウト/宛先到達不能パケットの送信が無効であることを示します。）

tracert 操作を開始する前に、送信元と宛先の間の中間デバイスで ICMP 宛先到達不能メッセージの送信を有効にする必要があります。次のいずれかの ICMP 宛先到達不能メッセージを受信すると、tracert 操作は停止します。

- !N −ネットワークに到達できません。
- !H −宛先ホストに到達できません。
- !P −プロトコルに到達できません。プロトコル番号は不明です。
- !F −フラグメンテーションが必要です。このメッセージは、パケットフラグメンテーションが必要であるが、即時デバイスに"Don't Fragment"ビットが設定されていることを示します。
- !W −宛先ホストが不明です。
- !Q −ToS でネットワークに到達できません。
- !T −ToS でホストに到達できません。
- !X −フィルタリングポリシーによって管理上禁止されている通信。
- !V −ホスト優先順位違反。
- !C −有効な優先順位カットオフ。

例

パケットが送信元から宛先（IP アドレス 1.1.2.2）へ向かうルートを表示します。

<AP> tracert 1.1.2.2

```
traceroute to 1.1.2.2 (1.1.2.2), 30 hops at most, 40 bytes each packet, press CTRL_C
to break
 1  1.1.1.2 (1.1.1.2) 673 ms 425 ms 30 ms
 2  1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms
```

表 1-2 コマンド出力

フィールド	説明
traceroute to 1.1.2.2(1.1.2.2)	現在の装置からIPアドレスが1.1.2.2の装置へ向かうIPパケットのルートを表示します。
hops at most	プローブパケットの最大Hop数です。このフィールドを表示する場合、**-m**を指定する必要があります。
bytes each packet	プローブパケットのバイト数です。

フィールド	説明
press CTRL_C to break	**tracert**コマンドを実行中、中止する場合、**Ctrl+C**を押下します。 エスケープキーは、**escape-key**コマンドを使用して設定できます。このコマンドの詳細については、コマンドマニュアルのセクション1の*基本機能“ログイン”*を参照してください。
2　1.1.2.2 (1.1.2.2) [AS 100] 580 ms 470 ms 80 ms	TTLが2のプローブパケットの結果です。2番目のホップは以下の情報が含まれます。 ● 最初のHopのドメイン名です。ドメイン名が設定されていない場合、IPアドレスが表示されます。 ● ホップのIPアドレスです。IPアドレスは括弧で表示されます。 ● ホップが所属しているAS番号です。指定したルーティングテーブルにホップがある場合のみAS番号が表示されます。 ● プローブパケットのラウンドトリップ時間です。 各プローブが送信したパケット数を表示する場合、**-q**を指定する必要があります。

目次

このセクションのページは **15-x-x** です。

2 章 NQA 2-1
2.1 NQA クライアント設定コマンド 2-1
2.1.1 advantage-factor 2-1
2.1.2 codec-type 2-2
2.1.3 data-fill 2-3
2.1.4 data-size 2-5
2.1.5 description 2-7
2.1.6 destination ip 2-8
2.1.7 destination port 2-9
2.1.8 display nqa history 2-10
2.1.9 display nqa result 2-12
2.1.10 display nqa statistics 2-23
2.1.11 frequency 2-31
2.1.12 history-record enable 2-32
2.1.13 history-record keep-time 2-33
2.1.14 history-record number 2-34
2.1.15 next-hop ip 2-34
2.1.16 nqa 2-35
2.1.17 nqa agent enable 2-37
2.1.18 nqa schedule 2-38
2.1.19 operation (FTP operation view) 2-39
2.1.20 operation (HTTP operation view) 2-41
2.1.21 password 2-42
2.1.22 probe count 2-43
2.1.23 probe packet-interval 2-45
2.1.24 probe packet-number 2-46
2.1.25 probe packet-timeout 2-47
2.1.26 probe timeout 2-48
2.1.28 reaction checked-element probe-fail (for trap) 2-51
2.1.29 reaction trap 2-52
2.1.30 resolve-target 2-53
2.1.31 route-option bypass-route 2-54
2.1.32 source interface (ICMP echo operation view/UDP tracert operation view) 2-56
2.1.33 source ip 2-58
2.1.34 source port 2-60
2.1.35 statistics hold-time 2-60

2.1.36 statistics interval 2-61
2.1.37 statistics max-group 2-63
2.1.38 tos 2-63
2.1.39 ttl 2-64
2.1.40 type 2-66
2.1.41 url 2-68
2.1.42 username 2-71
2.1.43 version 2-73
2.2 NQA サーバ設定コマンド 2-73
2.2.1 display nqa server 2-74
2.2.2 nqa server enable 2-76
2.2.3 nqa server tcp-connect 2-77
2.2.4 nqa server udp-echo 2-79

2章 NQA

2.1 NQAクライアント設定コマンド

2.1.1 advantage-factor

Syntax

advantage-factor *factor*

undo advantage-factor

デフォルト

0

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

factor: アドバンテージファクタを指定します。設定範囲は 0～20 です。

説明

advantage-factor コマンドは MOS（Mean Opinion Scores）値と ICPIF（Calculated Planning Impairment Factor）値をカウントするのに使用されるアドバンテージファクタを設定します。

undo advantage-factor コマンドはデフォルトに戻します。

音声品質の評価は、ユーザの音声品質の許容度に依存します。音声品質に高い許容度を持つユーザの場合、アドバンテージファクタの設定を行う **advantage-factor** コマンドを使用します。システムが ICPIF 値を計算する場合、音声品質の評価用に ICPIF と MOS の値を修正するため、アドバンテージファクタが取りはずされます。

例

音声テストのアドバンテージファクタを 10 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type voice

[AP-nqa-admin-test-voice] advantage-factor 10

2.1.2 codec-type

Syntax

codec-type { **g711a** | **g711u** | **g729a** }

undo codec-type

デフォルト

G.711 A-law

View

Voice operation view

定義済みユーザロール

network-admin

パラメータ

g711a: G.711 A-law コーデックタイプを指定します。

g711u: G.711 μ-law コーデックタイプを指定します。

g729a: G.729 A-law コーデックタイプを指定します。

説明

codec-type コマンドは音声テストのコーデックタイプを設定します。

undo codec-type コマンドはデフォルトに戻します。

例

音声テストのコーデックタイプを g729a に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type voice

[AP-nqa-admin-test-voice] codec-type g729a

2.1.3 data-fill

Syntax

data-fill *string* [**raw**]

undo data-fill

デフォルト

00010203040506070809

View

ICMP/UDP echo operation view

Path jitter/UDP jitter/voice operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

string: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

raw: ペイロードサイズに合わせて、切り捨てや繰り返しを行わずに、指定された payload fill string でパケットペイロードを埋めます。このキーワードは、UDP テンプレートビューでのみ使用できます。

説明

data-fill コマンドは各プローブパケットのペイロードに埋め込まれる文字列を設定します。

undo data-fill コマンドはデフォルトに戻します。

文字列の入力方法は、操作の種類によって異なります。

- ICMP エコーテストでは、設定された文字列は ICMP エコー要求の全ペイロードに埋め込まれます。
- UDP エコーテストでは、UDP パケットのペイロードの最初の 5 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- UDP ジッタテストでは、UDP パケットのペイロードの最初の 68 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。
- 音声テストでは、UDP パケットのペイロードの最初の 16 バイトは特定の用途に使用されます。設定された文字列はペイロードの残りの部分を埋め込むのに使用されます。

raw キーワードを指定すると、全ペイロードの文字列は指定されたとおりにパケットペイロードを埋めるために使用されます。
raw キーワードを指定しない場合、全ペイロードの文字列は最後に切り捨てられるか、プローブパケットのペイロードサイズに合わせて循環的に繰り返されます。
たとえば、ペイロードの塗りつぶし文字列を **abcd** に設定すると、次のようになります。

- ペイロードサイズが 3 バイトのプローブパケットは、abc で埋められます。
- ペイロードサイズが 6 バイトのプローブパケットは、adcdab で埋められます。

UDP テンプレートビューでは、**raw** キーワードが指定されていないプローブパケットに特殊文字が含まれています。QX シリーズ製品以外の宛先の装置の場合は、特殊文字が含まれていないプローブパケットのみを識別できるため、raw キーワードを指定します。クライアントで指定されたペイロード入力文字列が宛先の装置で識別できることを確認します。
宛先の装置が QX シリーズ製品の場合、殊文字を含むプローブパケットを識別できるため、raw キーワードは必須ではありません。raw キーワードは指定しないことを推奨します。

例

ICMP エコー要求のペイロードに埋め込まれる文字列 **abcd** を設定します。

```
<AP> system-view
[AP] nqa entry admin test
[AP-nqa-admin-test] type icmp-echo
[AP-nqa-admin-test-icmp-echo] data-fill abcd
```

2.1.4 data-size

Syntax

data-size *size*

undo data-size

デフォルト

異なるテストのプローブパケットのデフォルトのペイロードサイズを表 2-1 に示します。

表 2-1 プローブパケットのデフォルトのペイロードサイズ

テストタイプ	コーデックタイプ	デフォルトサイズ（バイト）
ICMP echo	—	100
UDP echo	—	100
UDP jitter	—	100
Path jitter	—	100
Voice	G.711 A-law	172
Voice	G.711 μ-law	172
Voice	G.729 A-law	32

View

ICMP/UDP echo operation view

UDP tracert operation view

Path jitter/UDP jitter/voice operation view

ICMP/UDP/tracert template view

定義済みユーザロール

network-admin

パラメータ

size: 各プローブパケットのペイロードサイズを指定します。以下に設定範囲を示します。

- ICMP エコーあるいは UDP エコーテストのプローブパケットの設定範囲は 20～65507 バイトです。
- UDP ジッタテストのプローブパケットの設定範囲は 68～65507 バイトです。
- 音声テストのプローブパケットの設定範囲は 16～65507 バイトです。

説明

data-size コマンドは各プローブパケットのペイロードサイズを設定します。

undo data-size コマンドはデフォルトに戻します。

ICMP エコーテストではコマンドは各エコー要求のペイロードサイズを設定します。

UDP エコーテスト、UDP ジッタ、音声テストではコマンドは各エコーUDP パケットのペイロードサイズを設定します。

例

各 ICMP エコー要求のペイロードサイズを 80 バイトに設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] data-size 80

ICMP テンプレートビューで、各プローブパケットのペイロードサイズを 80 バイトに設定します。

<AP> system-view

[AP] nqa template icmp icmptplt

[AP-nqatplt-icmp-icmptplt] data-size 80

2.1.5 description

Syntax

description *text*

undo description

デフォルト

設定なし

View

ICMP echo/UDP echo/TCP operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP operation view

UDP tracert operation view

ICMP jitter/UDP jitter/path jitter/voice operation view

すべての NQA operation view

定義済みユーザロール

network-admin

パラメータ

text: 文字列を指定します。設定範囲は 1～200 文字です。大文字、小文字を区別します。

説明

description コマンドはテストタイプや目的などの NQA テストの説明を設定します。

undo description コマンドは説明を削除します。

例

NQA テストの説明を **icmp-probe** に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] description icmp-probe

#ICMP テンプレートビューで、説明を NQA 操作の **icmp-probe** として設定します。

<AP> system-view

[AP] nqa template icmp icmptplt

[AP-nqatplt-icmp-icmptplt] description icmp-probe

2.1.6 destination ip

Syntax

destination ip *ip-address*

undo destination ip

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

ARP/DNS/ICMP/IMAP/POP3/RADIUS authentication/

RADIUS accounting/SMTP/SSL/TCP/TCP half open/UDP/WAP/tracert template view

定義済みユーザロール

network-admin

パラメータ

ip-address: テストの宛先 IPv4 アドレスを指定します。

説明

destination ip コマンドはテストの宛先 IPv4 アドレスを設定します。

undo destination ip コマンドは宛先 IPv4 アドレスを削除します。

例

ICMP エコーテストの宛先 IPv4 アドレスを 10.1.1.1 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] destination ip 10.1.1.1

ICMP テンプレートビューで、ICMP エコー動作の宛先 IPv 4 アドレスとして 10.1.1.1 を指定します。

<AP> system-view

[AP] nqa template icmp icmptplt

[AP-nqatplt-icmp-icmptplt] destination ip 10.1.1.1

2.1.7 destination port

Syntax

destination port *port-number*

undo destination port

デフォルト

UDP tracert 動作の宛先ポート番号：33434

他テスト：設定なし

NQA テンプレートの宛先ポート番号は次のとおりです。

- DNS テンプレート：53
- IMAP テンプレート：143
- POP 3 テンプレート：110
- RADIUS 認証テンプレート：1812
- RADIUS アカウンティングテンプレート：1813。
- SIP テンプレート：5060。
- SMTP テンプレート：25。
- WAP テンプレート：9201。
- tracert テンプレート：33434

他のタイプの NQA テンプレートには、宛先ポート番号は設定されません。

View

TCP/UDP echo operation view

UDP tracert operation view

UDP jitter/voice operation view

DNS/IMAP/POP3/RADIUS authentication/RADIUS accounting/SIP/SMTP/SSL/TCP/TCP half open /UDP/WAP/tracert template view

定義済みユーザロール

network-admin

パラメータ

port-number: テストの宛先ポート番号を指定します。設定範囲は 1～65535 です。

説明

destination port コマンドはテストの宛先ポート番号を設定します。

undo destination port コマンドは宛先ポート番号を削除します。

TCP ハーフオープンテンプレートの場合、このコマンドは **port-detect enable** コマンドが設定されている場合にのみ必要です。

例

UDP エコーテストの宛先ポート番号を 9000 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type udp-echo

[AP-nqa-admin-test-udp-echo] destination port 9000

#TCP テンプレートビューで、NQA 操作の宛先ポート番号を 9000 に設定します。

<AP> system-view

[AP] nqa template tcp tcptplt

[AP-nqatplt-tcp-tcptplt] destination port 9000

2.1.8 display nqa history

Syntax

display nqa history [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの履歴記録を表示します。

説明

display nqa history コマンドは NQA テストの履歴記録を表示します。

display nqa history コマンドは、次の操作の結果や統計情報を表示しません。

- ICMP ジッタ
- パスジッタ
- UDP ジッタ
- 音声

UDP ジッタテストと音声テストを確認する場合、**display nqa result** コマンドあるいは **display nqa statistics** コマンドを使用します。

例

管理者名が **administrator**、オペレーティングタグが **test** の NQA テストグループの履歴記録を表示します。

<AP> display nqa history administrator tracert

```
NQA entry (admin administrator, tag tracert) history records:
Index      TTL  Response  Hop IP         Status         Time
1          2    328       4.1.1.1        Succeeded      2013-09-09 14:46:06.2
1          2    328       4.1.1.1        Succeeded      2013-09-09 14:46:05.2
1          2    328       4.1.1.1        Succeeded      2013-09-09 14:46:04.2
1          1    328       3.1.1.2        Succeeded      2013-09-09 14:46:03.2
1          1    328       3.1.1.1        Succeeded      2013-09-09 14:46:02.2
1          1    328       3.1.1.1        Succeeded      2013-09-09 14:46:01.2
```

管理者名 **administrator** と操作タグ test で NQA 操作の履歴レコードを表示します。。

<AP> display nqa history administrator test

```
NQA entry (admin administrator, tag test) history records:
Index     Response     Status       Time
10        329          Succeeded    2011-04-29 20:54:26.5
9         344          Succeeded    2011-04-29 20:54:26.2
8         328          Succeeded    2011-04-29 20:54:25.8
7         328          Succeeded    2011-04-29 20:54:25.5
6         328          Succeeded    2011-04-29 20:54:25.1
5         328          Succeeded    2011-04-29 20:54:24.8
4         328          Succeeded    2011-04-29 20:54:24.5
3         328          Succeeded    2011-04-29 20:54:24.1
2         328          Succeeded    2011-04-29 20:54:23.8
1         328          Succeeded    2011-04-29 20:54:23.4
```

表 2-2 コマンド出力

フィールド	説明
Index	履歴記録のIDです。 1つのUDP tracert操作の履歴レコードは同じIDを持ちます。
TTL	プローブパケットのTTLです。
Response	テストが成功した場合、ラウンドトリップの時間を表示します。テストがタイムアウトしたとき、タイムアウト時間を表示します。テストが完了しない場合、**0**を表示します。単位はミリ秒です。
Hop IP	応答パケットを送信したノードのIPアドレスです。

フィールド	説明
Status	テスト結果の状態です。 ● **Succeeded**－成功しました。 ● **Unknown error**－未知のエラーです。(この状態は、NQA-Trackコラボレーションで Track状態スイッチオーバーをトリガーします。) ● **Internal error**－内部エラーです。(この状態は、NQA-Trackコラボレーションで Track状態スイッチオーバーをトリガーしません。) ● **Timeout**－タイムアウトしました。(この状態は、NQA-Trackコラボレーションで Track状態スイッチオーバーをトリガーします。)
Time	テストが完了したときの時間です。

2.1.9 display nqa result

Syntax

display nqa result [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの最新の結果を表示します。

説明

display nqa result コマンドは NQA テストの最新の結果を表示します。

例

管理者名 admin、テストタグ test の TCP テストの最新の結果を表示します。

<AP> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
```

```
  Send operation times: 1            Receive response times: 1
  Min/Max/Average round trip time: 35/35/35
  Square-Sum of round trip time: 1225
  Last succeeded probe time: 2011-05-29 10:50:33.2
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to disconnect: 0
  Failures due to no connection: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
```

管理者名 admin、テストタグ test の UDP ジッタテストの最新の結果を表示します。

<AP> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
   Send operation times: 10           Receive response times: 10
  Min/Max/Average round trip time: 15/46/26
  Square-Sum of round trip time: 8103
  Last packet received time: 2011-05-29 10:56:38.7
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
 UDP-jitter results:
  RTT number: 10
  Min positive SD: 8                 Min positive DS: 8
  Max positive SD: 18                Max positive DS: 8
  Positive SD number: 5              Positive DS number: 2
  Positive SD sum: 75                Positive DS sum: 32
  Positive SD average: 15            Positive DS average: 16
  Positive SD square-sum: 1189       Positive DS square-sum: 640
  Min negative SD: 8                 Min negative DS: 1
  Max negative SD: 24                Max negative DS: 30
  Negative SD number: 4              Negative DS number: 7
  Negative SD sum: 56                Negative DS sum: 99
  Negative SD average: 14            Negative DS average: 14
  Negative SD square-sum: 946        Negative DS square-sum: 1495
 One way results:
  Max SD delay: 22                   Max DS delay: 23
  Min SD delay: 7                    Min DS delay: 7
```

```
  Number of SD delay: 10              Number of DS delay: 10
  Sum of SD delay: 125                Sum of DS delay: 132
  Square-Sum of SD delay: 1805         Square-Sum of DS delay: 1988
  SD lost packets: 0                 DS lost packets: 0
  Lost packets for unknown reason: 0
```

管理者名 admin、テストタグ test の音声テストの最新の結果を表示します。

<AP> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
   Send operation times: 1000         Receive response times: 0
   Min/Max/Average round trip time: 0/0/0
   Square-Sum of round trip time: 0
   Last packet received time: 0-00-00 00:00:00.0
 Extended results:
   Packet loss ratio: 100%
   Failures due to timeout: 1000
   Failures due to internal error: 0
   Failures due to other errors: 0
   Packets out of sequence: 0
   Packets arrived late: 0
 Voice results:
  RTT number: 0
   Min positive SD: 0                 Min positive DS: 0
   Max positive SD: 0                 Max positive DS: 0
   Positive SD number: 0              Positive DS number: 0
   Positive SD sum: 0                 Positive DS sum: 0
   Positive SD average: 0             Positive DS average: 0
   Positive SD square-sum: 0          Positive DS square-sum: 0
   Min negative SD: 0                 Min negative DS: 0
   Max negative SD: 0                 Max negative DS: 0
   Negative SD number: 0              Negative DS number: 0
   Negative SD sum: 0                 Negative DS sum: 0
   Negative SD average: 0             Negative DS average: 0
   Negative SD square-sum: 0          Negative DS square-sum: 0
 One way results:
   Max SD delay: 0                   Max DS delay: 0
   Min SD delay: 0                   Min DS delay: 0
   Number of SD delay: 0              Number of DS delay: 0
   Sum of SD delay: 0                 Sum of DS delay: 0
   Square-Sum of SD delay: 0          Square-Sum of DS delay: 0
   SD lost packets: 0                 DS lost packets: 0
   Lost packets for unknown reason: 1000
 Voice scores:
```

```
   MOS value: 0.99                    ICPIF value: 87
```

#管理者名 **admin** および操作タグ **test** で、パスジッタ操作の最新の結果を表示します。

<AP> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
NQA entry (admin admin, tag test) test results:
 Hop IP 192.168.40.210
 Basic Results:
 Send operation times: 10
 Receive response times: 10
 Min/Max/Average round trip time: 1/1/1
 Square-Sum of round trip time: 10
 Extended Results:
 Packet loss ratio: 0%
 Failures due to timeout: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
 Packets out of sequence: 0
 Packets arrived late: 0
 Path-Jitter Results:
 Jitter number: 9
 Min/Max/Average jitter: 0/0/0
 Positive jitter number: 0
 Min/Max/Average positive jitter: 0/0/0
 Sum/Square-Sum positive jitter: 0/0
 Negative jitter number: 0
 Min/Max/Average negative jitter: 0/0/0
 Sum/Square-Sum negative jitter: 0/0
 Hop IP 192.168.50.209
 Basic Results:
 Send operation times: 10
 Receive response times: 10
 Min/Max/Average round trip time: 1/1/1
 Square-Sum of round trip time: 10
 Extended Results:
 Packet loss ratio: 0%
 Failures due to timeout: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
 Packets out of sequence: 0
 Packets arrived late: 0
 Path-Jitter Results:
 Jitter number: 9
```

```
 Min/Max/Average jitter: 0/0/0
 Positive jitter number: 0
 Min/Max/Average positive jitter: 0/0/0
 Sum/Square-Sum positive jitter: 0/0
 Negative jitter number: 0
 Min/Max/Average negative jitter: 0/0/0
 Sum/Square-Sum negative jitter: 0/0
```

#管理者名 **admin** および操作タグ **test** で、UDP tracert 操作の最新の結果を表示します。

<AP> display nqa result admin test

```
NQA entry (admin admin, tag test) test results:
 Send operation times: 6 Receive response times: 6
 Min/Max/Average round trip time: 35/35/35
 Square-Sum of round trip time: 1225
 Last succeeded probe time: 2013-09-09 14:23:24.5
 Extended results:
 Packet loss ratio: 0%
 Failures due to timeout: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
 UDP-tracert results:
 TTL Hop IP Time
 1 3.1.1.1 2013-09-09 14:23:24.5
 2 4.1.1.1 2013-09-09 14:23:24.5
```

表 2-3 コマンド出力

フィールド	説明
NQA entry (admin admin, tag test) test results	NQA操作結果です。
Data collecting in progress	テストの進捗状況です。
Path jitter result is not available	操作の結果は生成されません。
Send operation times	テスト数です。
Receive response times	受信した応答パケットの数です。
Min/Max/Average round trip time	最小/最大/平均ラウンドトリップタイムです。単位はミリ秒です。
Square-Sum of round trip time	ラウンドトリップタイムの2乗和です。
Last succeeded probe time	連続した最後のプローブが完了した時間です。テストでプローブが連続していない場合、0と表示されます。 このフィールドはUDPジッタ、音声テストで無効です。

フィールド	説明
Last packet received time	連続した最後の応答パケットを受信した時間です。プローブで応答パケットを受信しない場合、0と表示されます。 このフィールドはUDPジッタ、音声テストで有効です。
Extended results	拡張項目の結果です。
Packet loss ratio	平均パケット損失レートです。
Failures due to timeout	テストでタイムアウトが発生した回数です。
Failures due to disconnect	ピアが切断した数です。
Failures due to no connection	ピアとの接続に失敗した数です。
Failures due to internal error	内部エラーによる故障の数です。
Failures due to other errors	他のエラーによる故障の数です。
Packets out of sequence	異なる順番のパケットによる故障の数です。
ICMP-jitter results	ICMPジッタテスト結果です。 このフィールドはICMPジッタのみ有効です。
Packets arrived late	プローブがタイムアウトした後に受信した応答パケットの数です。
UDP-jitter results	UDPジッタテストの結果です。 このフィールドはUDPジッタテストのみ有効です。
Voice results	音声テストの結果です。 このフィールドは音声テストのみ有効です。
RTT number	応答パケットを受信した数です。
Min positive SD	送信元から宛先への最小ポジティブジッタです。
Min positive DS	宛先から送信元への最小ポジティブジッタです。
Max positive SD	送信元から宛先への最大ポジティブジッタです。
Max positive DS	宛先から送信元への最大ポジティブジッタです。
Positive SD number	送信元から宛先へのポジティブジッタの数です。
Positive DS number	宛先から送信元へのポジティブジッタの数です。
Positive SD sum	送信元から宛先へのポジティブジッタの合計数です。
Positive DS sum	宛先から送信元へのポジティブジッタの合計数です。

フィールド	説明
Positive SD average	送信元から宛先への平均ポジティブジッタです。
Positive DS average	宛先から送信元への平均ポジティブジッタです。
Positive SD square-sum	送信元から宛先へのポジティブジッタの2乗和です。
Positive DS square-sum	宛先から送信元へのポジティブジッタの2乗和です。
Min negative SD	送信元から宛先へのネガティブジッタの絶対値の最小値です。
Min negative DS	宛先から送信元へのネガティブジッタの絶対値の最小値です。
Max negative SD	送信元から宛先へのネガティブジッタの絶対値の最大値です。
Max negative DS	宛先から送信元へのネガティブジッタの絶対値の最大値です。
Negative SD number	送信元から宛先へのネガティブジッタの数です。
Negative DS number	宛先から送信元へのネガティブジッタの数です。
Negative SD sum	送信元から宛先へのネガティブジッタの絶対値の合計です。
Negative DS sum	宛先から送信元へのネガティブジッタの絶対値の合計です。
Negative SD average	送信元から宛先へのネガティブジッタの絶対値の平均です。
Negative DS average	宛先から送信元へのネガティブジッタの絶対値の平均です。
Negative SD square-sum	送信元から宛先へのネガティブジッタの2乗和です。
Negative DS square-sum	宛先から送信元へのネガティブジッタの2乗和です。
SD average	送信元から宛先へのジッタの平均値です。
DS average	宛先から送信元へのジッタの平均値です。
One way results	片方向遅延です。 このフィールドはUDPジッタテスト、音声テストで有効です。
Max SD delay	送信元から宛先への最大遅延です。
Max DS delay	宛先から送信元への最大遅延です。
Min SD delay	送信元から宛先への最小遅延です。

フィールド	説明
Min DS delay	宛先から送信元への最小遅延です。
Number of SD delay	送信元から宛先への遅延の数です。
Number of DS delay	宛先から送信元への遅延の数です。
Sum of SD delay	送信元から宛先への遅延の合計です。
Sum of DS delay	宛先から送信元への遅延の合計です。
Square-Sum of SD delay	送信元から宛先への遅延の2乗和です。
Square-Sum of DS delay	宛先から送信元への遅延の2乗和です。
SD lost packets	送信元から宛先への損失したパケット数です。
DS lost packets	宛先から送信元への損失したパケット数です。
Lost packets for unknown reason	不明な理由で損失したパケット数です。
Voice scores	音声パラメータです。 このフィールドは音声テストで有効です。
MOS value	音声テストの計算されたMOS値です。
ICPIF value	音声テストの計算されたICPIF値です。
Hop IP	ホップのIPアドレスです。 このフィールドは、パスジッタ動作でのみ使用できます。
Path-jitter results	パスジッタ動作の結果です。 このフィールドは、パスジッタ動作でのみ使用できます。
Jitter number	ジッタの数です。 このフィールドは、パスのジッタ操作でのみ使用できます。
Min/Max/Average jitter	最小/最大/平均ジッタ（ミリ秒単位）。 このフィールドは、パスジッタ動作でのみ使用できます。
Positive jitter number	正のジッタの数です。 このフィールドは、パスジッタ動作でのみ使用できます。
Min/Max/Average positive jitter	ミリ秒単位の最小/最大/平均正のジッタです。 このフィールドは、パスジッタ動作でのみ使用できます。
Sum/Square-Sum positive jitter	正のジッタの合計/平方和です。 このフィールドは、パスジッタ操作でのみ使用できます。
Negative jitter number	負のジッタの数です。 このフィールドは、パスジッタ動作でのみ使用できます。
Min/Max/Average negative jitter	ミリ秒単位の最小/最大/平均負ジッタです。 このフィールドは、パスジッタ動作でのみ使用できます。

フィールド	説明
Sum/Square-Sum negative jitter	負のジッタの数です。 このフィールドは、パスジッタ動作でのみ使用できます。
TTL	受信した応答パケットのTTLです。 ルーティングテーブルバイパス機能の動作が無効の場合、このフィールドにはプローブパケットのTTL値が表示されます。 ルーティングテーブルバイパス機能が有効の場合、このフィールドの値は**init-ttl**コマンドによって異なります。ただし、プローブパケット内の実際のTTL値は1に固定されています。
Hop IP	送信した応答パケットのノードのIPアドレスです。
Time	NQAクライアントが応答パケットを受信した時間です。
Status	Y.1564オペレーションまたはY.1564オペレーション内のテストのステータス。 値は次のいずれかになります。 • **Succeeded**—成功しました。 • **Failed**—失敗しました。 • **In progress**—進行中です。 • **Aborted**—テストは手動で中止されました。 • **Timeout**—タイムアウトしました。 • **Unknown error**—未知のエラーです。 このフィールドには、ステータスが無意味なテストの2つのハイフン(--)が表示されます。
Last test	最後に完了したテストです。 値は次のとおりです。 • **CIR test** • **PIR test** • **Traffic policing test** • **Service performance test**
Estimated total time	Y.1564操作にかかると推定された合計時間 (秒単位) です。
Actual test time used	Y.1564操作の完了にかかった実際の時間 (秒単位) です。 テスト開始時間と終了時間の測定に使用されるタイマは、1秒の精度です。そのため、このフィールドに表示される値と、テスト開始から終了までの時間との間に最大1秒の差が存在する可能性があります。
CIR test (with the step of 1)	ステップ数が1のCIRテストに関する情報です。 CIRテストのステップ数は、1から1000の範囲の任意の値に設定できます。

フィールド	説明
Start time	テストの開始時刻です。
End time	テストの終了時刻です。
Min/Max/Average IR(Kbps)	最小、最大、および平均情報レート (kbps単位) です 。
Min/Max/Average FTD(us)	最小、最大、および平均フレーム転送遅延 (μs単位) です。
Min/Max/Average FDV(us)	最小、最大、および平均フレーム遅延変動 (μs単位) です。
FL count/FLR	失われたフレーム数とフレーム損失率です。
Packets out of order	順不同のパケット数です。
Severely Err Secs/AVAIL	重度エラー秒 (SES) の合計数とネットワーク可用性比 (AVAIL)です。 1秒間隔のフレーム損失率が50%を超えると、重大なエラー秒が発生します。 AVAILは次のように計算されます。AVAIL=使用可能な期間の合計秒数/テストにかかった合計秒数です。 ● 連続して10個のSESが記録された後、ネットワークが使用不能期間にあります。使用不能期間は、連続して10個の非SESが記録された時点で終了します。 ● 非SESが10回連続した後、ネットワークは使用可能な期間にあります。使用可能な期間は、SESが10回連続して記録された時点で終了します。 デフォルトでは、テストは使用可能な期間に開始されると見なされます。
PIR test (color green)	PIRテストの緑色のフレームに関する統計情報です。
PIR test (color yellow)	PIRテストの黄色のフレームに関する統計情報です。
PIR test (total)	PIRテストに関する統計情報の概要です。
PIR test (color-blind)	非色認識モードでのPIRテストに関する統計情報です。
Traffic policing test (color green)	トラフィックポリシングテストの緑色のフレームに関する統計情報です。
Traffic policing test (color yellow)	トラフィックポリシングテストの黄色のフレームに関する統計情報です。
Traffic policing test (total)	トラフィックポリシングテストに関する統計情報の要約です。
Traffic policing test (color-blind)	非カラー対応モードのトラフィックポリシングテストに関する統計情報です。

フィールド	説明
Service performance test	サービスパフォーマンステストに関する統計情報です。
Basic results	基本的な項目の結果です。
Min-jitter(ns)	ナノ秒単位の最小ジッタです。
Max-jitter(ns)	ナノ秒単位の最大ジッタです。
Avg-jitter(ns)	ナノ秒単位の平均ジッタです。
Sent packets	送信パケット数です。
Received packets	受信パケット数です。

2.1.10 display nqa statistics

Syntax

display nqa statistics [*admin-name operation-tag*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はテストタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。NQA テストを指定しない場合、すべての NQA テストの統計情報を表示します。

説明

display nqa statistics コマンドは NQA テストの統計情報を表示します。

NQA テストが完了した後、統計情報が作成されます。テストが完了する前に **display nqa statistics** コマンドを実行した場合、統計情報はすべて 0 で表示されます。

reaction entry が設定されている場合、**statistics interval** コマンドで指定された期間、リ reaction entry をモニタリングした結果を表示します。以下の場合、ハイフン（-）が結果として表示されます。

- しきい値タイプが平均値
- 音声テストのモニタリングが ICPIF あるいは MOS

NQA 操作を指定しない場合、このコマンドはすべての NQA 操作の統計情報を表示します。

例

管理者名 admin、テストタグ test の TCP テストの統計情報を表示します。

<AP> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:30:20.0
    Life time: 2 seconds
    Send operation times: 1            Receive response times: 1
    Min/Max/Average round trip time: 13/13/13
    Square-Sum of round trip time: 169
```

```
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to disconnect: 0
    Failures due to no connection: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
```

管理者名 admin、テストタグ test の UDP ジッタテストの統計情報を表示します。

<AP> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
  NO. : 1
    Start time: 2007-01-01 09:33:22.3
    Life time: 23 seconds
    Send operation times: 100          Receive response times: 100
    Min/Max/Average round trip time: 1/11/5
    Square-Sum of round trip time: 24360
  Extended results:
    Packet loss ratio: 0%
    Failures due to timeout: 0
    Failures due to internal error: 0
    Failures due to other errors: 0
    Packets out of sequence: 0
    Packets arrived late: 0
  UDP-jitter results:
   RTT number: 550
    Min positive SD: 1                 Min positive DS: 1
    Max positive SD: 7                 Max positive DS: 1
    Positive SD number: 220             Positive DS number: 97
    Positive SD sum: 283               Positive DS sum: 287
    Positive SD average: 1              Positive DS average: 2
    Positive SD square-sum: 709         Positive DS square-sum: 1937
    Min negative SD: 2                 Min negative DS: 1
    Max negative SD: 10                Max negative DS: 1
    Negative SD number: 81              Negative DS number: 94
    Negative SD sum: 556               Negative DS sum: 191
    Negative SD average: 6              Negative DS average: 2
    Negative SD square-sum: 4292         Negative DS square-sum: 967
  One way results:
    Max SD delay: 5                    Max DS delay: 5
    Min SD delay: 1                    Min DS delay: 1
    Number of SD delay: 550             Number of DS delay: 550
    Sum of SD delay: 1475               Sum of DS delay: 1201
```

```
  Square-Sum of SD delay: 5407          Square-Sum of DS delay: 3959
  SD lost packets: 0                  DS lost packets: 0
  Lost packets for unknown reason: 0
 Reaction statistics:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      jitter-DS       accumulate      90           25
  2      jitter-SD       average         -            -
  3      OWD-DS          -               100          24
  4      OWD-SD          -               100          13
  5      packet-loss     accumulate      0            0
  6      RTT             accumulate      100          52
```

管理者名 admin、テストタグ test の音声テストの統計情報を表示します。

<AP> display nqa statistics admin test

```
NQA entry (admin admin, tag test) test statistics:
 NO. : 1
  Start time: 2007-01-01 09:33:45.3
  Life time: 120 seconds
  Send operation times: 10            Receive response times: 10
  Min/Max/Average round trip time: 1/12/7
  Square-Sum of round trip time: 620
 Extended results:
  Packet loss ratio: 0%
  Failures due to timeout: 0
  Failures due to internal error: 0
  Failures due to other errors: 0
  Packets out of sequence: 0
  Packets arrived late: 0
 Voice results:
  RTT number: 10
  Min positive SD: 3                  Min positive DS: 1
  Max positive SD: 10                 Max positive DS: 1
  Positive SD number: 3               Positive DS number: 2
  Positive SD sum: 18                 Positive DS sum: 2
  Positive SD average: 6              Positive DS average: 1
  Positive SD square-sum: 134         Positive DS square-sum: 2
  Min negative SD: 3                  Min negative DS: 1
  Max negative SD: 9                  Max negative DS: 1
  Negative SD number: 4               Negative DS number: 2
  Negative SD sum: 25                 Negative DS sum: 2
  Negative SD average: 6              Negative DS average: 1
  Negative SD square-sum: 187         Negative DS square-sum: 2
 One way results:
```

```
  Max SD delay: 0                    Max DS delay: 0
  Min SD delay: 0                    Min DS delay: 0
  Number of SD delay: 0               Number of DS delay: 0
  Sum of SD delay: 0                 Sum of DS delay: 0
  Square-Sum of SD delay: 0           Square-Sum of DS delay: 0
  SD lost packets: 0                 DS lost packets: 0
  Lost packets for unknown reason: 0
Voice scores:
  Max MOS value: 4.40                Min MOS value: 4.40
  Max ICPIF value: 0                 Min ICPIF value: 0
Reaction statistics:
  Index  Checked Element  Threshold Type  Checked Num  Over-threshold Num
  1      ICPIF            -              -            -
  2      MOS              -              -            -
```

表 2-4 コマンド出力

フィールド	説明
No.	統計情報のグループIDです。
Start time	テストが開始した時間です。
Life time	テストの所要時間です。
Send operation times	送信したプローブパケットの数です。
Receive response times	受信した応答パケットの数です。
Min/Max/Average round trip time	最小/最大/平均ラウンドトリップタイムです。単位はミリ秒です。
Square-Sum of round trip time	ラウンドトリップタイムの2乗和です。
Packet loss ratio	平均パケット損失レートです。
Failures due to timeout	テストでタイムアウトが発生した回数です。
Failures due to disconnect	ピアが切断した数です。
Failures due to no connection	ピアとの接続に失敗した数です。
Failures due to internal error	内部エラーによる故障の数です。
Failures due to other errors	他のエラーによる故障の数です。
Packets out of sequence	異なる順番のパケットによる故障の数です。

フィールド	説明
Packets arrived late	プローブがタイムアウトしたのち応答パケットを受信した数です。
ICMP-jitter results	ICMPジッタ動作の結果。 このフィールドは、ICMPジッタ動作でのみ使用できます。
UDP-jitter results	UDPジッタテストの結果です。このフィールドはUDPジッタテストのみ有効です。
Voice results	音声テストの結果です。このフィールドは音声テストのみ有効です。
RTT number	応答パケットを受信した数です。
Min positive SD	送信元から宛先への最小ポジティブジッタです。
Min positive DS	宛先から送信元への最小ポジティブジッタです。
Max positive SD	送信元から宛先への最大ポジティブジッタです。
Max positive DS	宛先から送信元への最大ポジティブジッタです。
Positive SD number	送信元から宛先へのポジティブジッタの数です。
Positive DS number	宛先から送信元へのポジティブジッタの数です。
Positive SD sum	送信元から宛先へのポジティブジッタの合計数です。
Positive DS sum	宛先から送信元へのポジティブジッタの合計数です。
Positive SD average	送信元から宛先への平均ポジティブジッタです。
Positive DS average	宛先から送信元への平均ポジティブジッタです。
Positive SD square-sum	送信元から宛先へのポジティブジッタの2乗和です。
Positive DS square-sum	宛先から送信元へのポジティブジッタの2乗和です。
Min negative SD	送信元から宛先へのネガティブジッタの絶対値の最小値です。
Min negative DS	宛先から送信元へのネガティブジッタの絶対値の最小値です。
Max negative SD	送信元から宛先へのネガティブジッタの絶対値の最大値です。
Max negative DS	宛先から送信元へのネガティブジッタの絶対値の最大値です。
Negative SD number	送信元から宛先へのネガティブジッタの数です。

フィールド	説明
Negative DS number	宛先から送信元へのネガティブジッタの数です。
Negative SD sum	送信元から宛先へのネガティブジッタの絶対値の合計です。
Negative DS sum	宛先から送信元へのネガティブジッタの絶対値の合計です。
Negative SD average	送信元から宛先へのネガティブジッタの絶対値の平均です。
Negative DS average	宛先から送信元へのネガティブジッタの絶対値の平均です。
Negative SD square-sum	送信元から宛先へのネガティブジッタの2乗和です。
Negative DS square-sum	宛先から送信元へのネガティブジッタの2乗和です。
SD average	送信元から宛先へのジッタの平均値です。
DS average	宛先から送信元へのジッタの平均値です。
One way results	片方向遅延です。 このフィールドはUDPジッタテスト、音声テストで有効です。
Max SD delay	送信元から宛先への最大遅延です。
Max DS delay	宛先から送信元への最大遅延です。
Min SD delay	送信元から宛先への最小遅延です。
Min DS delay	宛先から送信元への最小遅延です。
Number of SD delay	送信元から宛先への遅延の数です。
Number of DS delay	宛先から送信元への遅延の数です。
Sum of SD delay	送信元から宛先への遅延の合計です。
Sum of DS delay	宛先から送信元への遅延の合計です。
Square-Sum of SD delay	送信元から宛先への遅延の2乗和です。
Square-Sum of DS delay	宛先から送信元への遅延の2乗和です。
SD lost packets	送信元から宛先への損失したパケット数です。
DS lost packets	宛先から送信元への損失したパケット数です。
Lost packets for unknown reason	不明な理由で損失したパケット数です。

フィールド	説明
Voice scores	音声パラメータです。 このフィールドは音声テストで有効です。
Max MOS value	最大MOS値です。
Min MOS value	最小MOS値です。
Max ICPIF value	最大ICPIF値です。
Min ICPIF value	最小ICPIF値です。
Reaction statistics	カウント期間中のreaction entryに関する統計情報です。
Index	reaction entryのIDです。
Checked Element	モニタリングされる要素です。
Threshold Type	しきい値タイプです。
Checked Num	データ収集用にモニタリングされているターゲット数です。
Over-threshold Num	しきい値違反の数です。
Path	パスジッタ動作でのパスのシリアル番号です。 このフィールドは、パスジッタ動作でのみ使用できます。
Hop IP	ホップのIPアドレスです。 このフィールドは、パスジッタ動作でのみ使用できます。
Path-jitter results	パスジッタ動作の結果です。 このフィールドは、パスジッタ動作でのみ使用できます。
Jitter number	ジッタの数です。 このフィールドは、パスのジッタ操作でのみ使用できます。
Min/Max/Average jitter	最小/最大/平均ジッタ（ミリ秒単位）。 このフィールドは、パスジッタ動作でのみ使用できます。
Positive jitter number	正のジッタの数です。 このフィールドは、パスジッタ動作でのみ使用できます。
Min/Max/Average positive jitter	ミリ秒単位の最小/最大/平均正のジッタです。 このフィールドは、パスジッタ動作でのみ使用できます。
Sum/Square-Sum positive jitter	正のジッタの合計/平方和です。 このフィールドは、パスジッタ操作でのみ使用できます。
Negative jitter number	負のジッタの数です。 このフィールドは、パスジッタ動作でのみ使用できます。
Min/Max/Average negative jitter	ミリ秒単位の最小/最大/平均負ジッタです。 このフィールドは、パスジッタ動作でのみ使用できます。
Sum/Square-Sum negative jitter	負のジッタの数です。 このフィールドは、パスジッタ動作でのみ使用できます。

表 2-5 に DHCP/DLSw/DNS/FTP/HTTP/SNMP/TCP/UDP エコーテストのしきい値モニタリングフィールドの説明を示します。

表 2-5 DHCP/DLSw/DNS/FTP/HTTP/SNMP/TCP/UDP エコーテストのしきい値モニタリングフィールドの説明

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
probe-duration	accumulate	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
	average	ー	ー	ー
	consecutive	カウント期間のプローブ	完了したプローブ数	カウント期間中にしきい値を超過したプローブ数
probe-fail	accumulate	カウント期間のプローブ	完了したプローブ数	プローブ失敗数
	consecutive	カウント期間のプローブ	完了したプローブ数	プローブ失敗数

表 2-6 にUDP ジッタ/音声テストのしきい値モニタリングフィールドの説明を示します。

表 2-6 UDP ジッタ/音声テストのしきい値モニタリングフィールドの説明

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
RTT	accumulate	カウント期間のプローブ	送信したパケット数	ラウンドトリップ中にしきい値を超過したパケット数
	average	ー	ー	ー
jitter-DS/jitter-SD	accumulate	カウント期間のプローブ	送信したパケット数	1方向ジッタ時間中にしきい値を超過したパケット数
	average	ー	ー	ー
OWD-DS/OWD-SD	ー	カウント期間のプローブ	送信したパケット数	1方向ジッタ時間中にしきい値を超過したパケット数

モニタリングされる性能メトリック	しきい値タイプ	収集データ	モニタリングされているターゲット数	しきい値違反数
packet-loss	accumulate	カウント期間のプローブ	送信したパケット数	パケット損失数
ICPIF/MOS（音声テストのみ有効）	―	―	―	―

関連コマンド

statistics interval

2.1.11 frequency

Syntax

frequency *interval*

undo frequency

デフォルト

2 つの連続する音声テスト間隔は 60000 ミリ秒です。他のテストの 2 つの連続するテスト間隔は 0 ミリ秒です。

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

interval: 2 つの連続するテスト間隔を指定します。設定範囲は 0～604800000 ミリ秒です。0 を指定した場合、テストは 1 回だけ実行され、統計情報は作成しません。

説明

frequency コマンドは NQA テストを繰り返す間隔を設定します。

undo frequency コマンドはデフォルトに戻します。

テスト間隔になってもテストが完了しないとき、次のテストが開始します。

例

ICMP エコーテストを繰り返す間隔を 1000 ミリ秒に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] frequency 1000

2.1.12 history-record enable

Syntax

history-record enable

undo history-record enable

デフォルト

有効

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

定義済みユーザロール

network-admin

説明

history-record enable コマンドは NQA テストの履歴記録を保存することを有効にします。

undo history-record enable コマンドは NQA テストの履歴記録を保存することを無効にします。

NQA テストの履歴記録を表示する場合、**display nqa history** コマンドを使用します。

undo history-record enable コマンドは NQA テストの既存の履歴記録も削除します。

例

NQA テストの履歴記録を保存することを有効にします。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] history-record enable

関連コマンド

display nqa history

2.1.13 history-record keep-time

Syntax

history-record keep-time *keep-time*

undo history-record keep-time

デフォルト

120 分

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

定義済みユーザロール

network-admin

パラメータ

keep-time: 履歴記録を保存する期間を指定します。設定範囲は 1～1440 分です。

説明

history-record keep-time コマンドは NQA テストの履歴記録の有効期限を指定します。

undo history-record keep-time コマンドはデフォルトに戻します。

NQA テストが完了したとき、タイマが開始します。すべての記録は有効期限になったとき、削除されます。

例

ICMP エコーテストの履歴記録の有効期限を 100 分に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] history-record keep-time 100

2.1.14 history-record number

Syntax

history-record number *number*

undo history-record number

デフォルト

50

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

定義済みユーザロール

network-admin

パラメータ

number: NQA テストで履歴記録を保存できる最大数を指定します。設定範囲は 0〜50 です。

説明

history-record number コマンドは NQA テストで履歴記録を保存できる最大数を設定します。

undo history-record number コマンドはデフォルトに戻します。

NQA テストの履歴記録の数が最大数を超過した場合、もっとも古い履歴記録が削除されます。

例

ICMP エコーテストで履歴記録を保存できる最大数を 10 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] history-record number 10

2.1.15 next-hop ip

Syntax

next-hop ip *ip-address*

undo next-hop ip

デフォルト

設定なし

View

ICMP echo operation view

DNS/ICMP/TCP half open template view

定義済みユーザロール

network-admin

パラメータ

ip-address: ネクストホップの IP アドレスを指定します。

説明

next-hop コマンドは ICMP エコーテストのネクストホップの IP アドレスを設定します。

undo next-hop コマンドはネクストホップの IP アドレスを削除します。

ネクストホップの IP アドレスが設定されていない場合、装置は ICMP エコーパケットのネクストホップの IP アドレスを決定するためルーティングテーブルを検索します。

例

ICMP エコーテストのネクストホップの IP アドレスを 10.1.1.1 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.1

2.1.16 nqa

Syntax

nqa entry *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

all: すべての NQA テストを削除します。

説明

nqa コマンドは NQA テストを作成し、その view に移行します。NQA テストがすでに存在する場合、その view に移行します。

undo nqa コマンドはテストを削除します。

例

管理者 **admin** とテストタグ **test** の NQA テストを作成し、NQA operation view に移行します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test]

2.1.17 nqa agent enable

Syntax

nqa agent enable

undo nqa agent enable

デフォルト

有効

View

System view

定義済みユーザロール

network-admin

説明

nqa agent enable コマンドは NQA クライアントを有効にします。

undo nqa agent enable コマンドは NQA クライアントを無効にし、すべてのテストを停止します。

例

NQA クライアントを有効にします。

<AP> system-view

[AP] nqa agent enable

関連コマンド

nqa server enable

2.1.18 nqa schedule

Syntax

nqa schedule *admin-name operation-tag* **start-time** { *hh:mm:ss* [*yyyy/mm/dd* | *mm/dd/yyyy*] | **now** } **lifetime** { *lifetime* | **forever** } [**recurring**]

undo nqa schedule *admin-name operation-tag*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

admin-name operation-tag: 管理者名とテストタグで NQA テストを指定します。*admin-name* は NQA テストを作成する管理者の名前を示します。*operation-tag* はオペレーションタグを示します。*admin-name*、*operation-tag* の設定範囲は 1～32 文字です。大文字、小文字を区別しません。ハイフン（-）を使用することができません。

start-time: NQA テストの開始日時を指定します。

hh:mm:ss: NQA テストの開始時間を指定します。

yyyy/mm/dd: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

mm/dd/yyyy: NQA テストの開始日を指定します。デフォルトは現在のシステム時間です。yyy の設定範囲は 2000～2035 です。

now: すぐにテストを開始します。

lifetime: テストの有効期限を指定します。

lifetime: 動作期間を指定します。設定範囲は 1～2147483647 秒です。

forever: **undo nqa schedule** コマンドを使用して手動で停止するまでテストを実行します。

recurring: 開始時間に自動でテストを開始し、指定した期間、実行し続けます。指定しない場合、指定した期間で 1 回のみ実行します。

説明

nqa schedule コマンドは NQA テストのスケジューリングのパラメータを設定します。

undo nqa schedule コマンドはテストを停止します。

NQA テストは開始日時と終了日時（開始日時＋動作期間）で動作します。開始日時がシステム時間より前である場合、テストはすぐさま開始します。開始日時と終了日時の両方がシステム時間より前である場合、テストは開始しません。現在のシステム時間を表示する場合、**display clock** コマンドを使用します。

スケジュールされた NQA テストの operation view あるいは operation type view に移行することはできません。

例

管理者 **admin** とテストタグ **test** の NQA テストをスケジューリングします。2008 年 8 月 8 日の 08 時 08 分 08 秒に開始し、1000 秒間テストを行うように設定します。

<AP> system-view

[AP] nqa schedule admin test start-time 08:08:08 2008/08/08 lifetime 1000 recurring

関連コマンド

- **destination ip**
- **display clock**（コマンドマニュアルのセクション 2 *システム管理　“装置管理”*）
- **nqa entry**
- **type**

2.1.19 operation (FTP operation view)

Syntax

operation { **get** | **put** }

undo operation

デフォルト

get

View

FTP operation view

定義済みユーザロール

network-admin

パラメータ

get: FTP サーバからファイルを取得します。

put: FTP サーバにファイルを転送します。

説明

operation コマンドは FTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

filename コマンドで **put** オペレーションを実行するとき、NQA クライアント上にファイルが存在していることを確認してください。

FTP サーバからファイルを取得する場合、FTP サーバの URL に指定されたファイルが存在していることを確認してください。NQA クライアントは FTP サーバから取得したファイルを保存しません。

FTP テストではファイルサイズが小さいファイルを使用してください。大きいサイズのファイルは、タイムアウトでテストが失敗したり、ネットワークの帯域幅以上を独占して他のサービスに影響を与えたりする可能性があります。

例

FTP テストのオペレーションタイプを **put** に指定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type ftp

[AP-nqa-admin-test-ftp] operation put

関連コマンド

- **password**
- **username**

2.1.20 operation (HTTP operation view)

Syntax

operation { **get** | **post** | **raw** }

undo operation

デフォルト

get

View

HTTP operation view

定義済みユーザロール

network-admin

パラメータ

get: HTTP サーバからファイルを取得します。

post: HTTP サーバにファイルを転送します。

raw : HTTP サーバに RAW 要求を送信します。

説明

operation コマンドは HTTP テストのオペレーションタイプを指定します。

undo operation コマンドはデフォルトに戻します。

HTTP テストはプローブパケットとして HTTP 要求を使用します。

HTTP の **get** あるいは **post** オペレーションの HTTP 要求の内容は **url** コマンドによって指定された URL から取得されます。

raw 操作の場合、要求の内容は raw 要求ビューで設定されます。**raw-request** コマンドを使用すると、raw request view に入ることができます。

例

HTTP テストのオペレーションのタイプを **raw** に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type http

[AP-nqa-admin-test-http] operation raw

HTTP テンプレートビューで HTTP テストのオペレーションのタイプを **raw** に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] nqa template http httptplt

[AP -nqatplt-http-httptplt] operation raw

関連コマンド

- **password**
- **username**

2.1.21 password

Syntax

password { **cipher** | **simple** } *string*

undo password

デフォルト

設定なし

View

FTP/HTTP operation view

FTP/HTTP/HTTPS/IMAP/POP3/RADIUS authentication template view

定義済みユーザロール

network-admin

パラメータ

cipher: 暗号パスワードを指定します。

simple: プレーンパスワードを指定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは暗号テキストで保存されます。

string: パスワードを指定します。大文字、小文字を区別します。**simple** を指定した場合の設定範囲は 1～32 文字です。**cipher** を指定した場合の設定範囲は 1～73 文字です。

- FTP、HTTP、および HTTPS 操作の場合、パスワードのプレーン形式は 1～32 文字の大文字と小文字を区別する文字列です。パスワードの暗号化形式は、1～73 文字の大文字と小文字を区別する文字列です。
- RADIUS テンプレートの場合、パスワードのプレーン形式は、1～64 文字の大文字と小文字を区別する文字列です。パスワードの暗号化形式は、1～117 文字の大文字と小文字を区別する文字列です。
- IMAP および POP 3 テンプレートの場合、パスワードのプレーン形式は 1～40 文字の文字列です。パスワードの暗号化形式は 1～85 文字の文字列です。

説明

password コマンドは FTP あるいは HTTP ログインパスワードを設定します。

undo password コマンドは設定を削除します。

例

FTP ログインパスワードを **ftpuser** に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type ftp

[AP-nqa-admin-test-ftp] password simple ftpuser

FTP テンプレートビューで FTP ログインパスワードを **ftpuser** に設定します

<AP> system-view

[AP] nqa template ftp ftptplt

[AP-nqatplt-ftp-ftptplt] password simple ftpuser

関連コマンド

- **operation**
- **username**

2.1.22 probe count

Syntax

probe count *times*

undo probe count

デフォルト

1

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter operation view

ICMP jitter/UDP jitter operation view

定義済みユーザロール

network-admin

パラメータ

times: NQA テスト（プローブ）の検査回数を指定します。設定範囲は 1～15 です。

- UDP tracert 操作の場合、この引数はパスに沿った各ホップへのプローブの時間を指定します。この引数の値の範囲は 1～10 です。
- 他のタイプの操作の場合、この引数は操作ごとに宛先へのプローブの時間を指定します。この引数の値の範囲は 1～15 です。

説明

probe count コマンドは NQA テストの検査回数を設定します。

undo probe count コマンドはデフォルトに戻します。

以下に異なるタイプのテストを実行する方法を示します。

- TCP あるいは DLSw テストは接続を設定します。
- UDP ジッタテストは多くのプローブパケットを送信します。多くのプローブパケットは **probe packet-number** コマンドによって設定されます。
- FTP テストはファイルをアップロードあるいはダウンロードします。
- HTTP テストは Web ページを取得します。
- DHCP テストは DHCP を介して IP アドレスを取得します。
- DNS テストはドメイン名を IP アドレスに変換します。
- ICMP エコーテストは ICMP エコー要求を送信します。
- UDP エコーテストは UDP パケットを送信します。
- SNMP テストは 1 つの SNMPv1 パケット、1 つの SNMPv2c パケット、1 つの SNMPv3 パケットを送信します。

テストが複数のプローブを実行する場合、NQA クライアントは以下の状況で新しいプローブを開始します。

- NQA クライアントが最後のプローブで送信したパケットの応答を受信します。
- プローブのタイムアウト時間が終了します。

このコマンドは、音声またはパスジッタ操作では使用できません。これらの各操作は、1 つのプローブだけを実行します。

例

ICMP エコーテストを実行する検査回数を 10 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] probe count 10

2.1.23 probe packet-interval

Syntax

probe packet-interval *interval*

undo probe packet-interval

デフォルト

20 ミリ秒

View

ICMP jitter/path jitter/UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

interval: パケットを送信する間隔を指定します。設定範囲は 10～60000 ミリ秒です。

説明

probe packet-interval コマンドはプローブのパケットを送信する間隔を設定します。

undo probe packet-interval コマンドはデフォルトに戻します。

例

UDP ジッタテストのパケットを送信する間隔を 100 ミリ秒に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type udp-jitter

[AP-nqa-admin-test-udp-jitter] probe packet-interval 100

2.1.24 probe packet-number

Syntax

probe packet-number *packet-number*

undo probe packet-number

デフォルト

UDP ジッタテストは 10 のパケットを送信します。音声テストは 1000 のパケットを送信します。

View

ICMP jitter/path jitter/UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

packet-number: プローブごとに送信するパケット数を指定します。

- UDP ジッタテストの設定範囲は 10～1000 です。
- 音声テストの設定範囲は 10～60000 です。

説明

probe packet-number コマンドは UDP ジッタテスト、音声テストで送信するパケットの数を設定します。

undo probe packet-number コマンドはデフォルトに戻します。

例

UDP ジッタテストで 100 パケットを送信するように設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type udp-jitter

[AP-nqa-admin-test-udp-jitter] probe packet-number 100

2.1.25 probe packet-timeout

Syntax

probe packet-timeout *timeout*

undo probe packet-timeout

デフォルト

UDP ジッタテストの応答タイムアウト時間は 3000 ミリ秒です。

音声テストの応答タイムアウト時間は 5000 ミリ秒です。

View

ICMP jitter/path jitter/UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

timeout: UDP ジッタテスト、音声テストの応答を待つタイムアウト時間を指定します。設定範囲は 10～3600000 ミリ秒です。

説明

probe packet-timeout コマンドは UDP ジッタテスト、音声テストの応答を待つタイムアウト時間を設定します。

undo probe packet-timeout コマンドはデフォルトに戻します。

例

UDP ジッタテストの応答を待つタイムアウト時間を 100 ミリ秒に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type udp-jitter

[AP-nqa-admin-test-udp-jitter] probe packet-timeout 100

2.1.26 probe timeout

Syntax

probe timeout *timeout*

undo probe timeout

デフォルト

3000 ミリ秒

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP tracert operation view

Any NQA template view

定義済みユーザロール

network-admin

パラメータ

timeout: プローブのタイムアウト時間を指定します。

- FTP テスト、HTTP テストの設定範囲は 10～86400000 ミリ秒です。
- DHCP テスト、DNS テスト、DLSw テスト、ICMP エコーテスト、TCP テスト、UDP エコーテストおよび UDP tracert テストの設定範囲は 10～3600000 ミリ秒です。
- FTP、HTTP、および HTTPS テンプレートの場合、値の範囲は 10 から 86400000 です。
- その他のタイプの NQA テンプレートの場合、値の範囲は 10 から 3600000 です。

説明

probe timeout コマンドはプローブのタイムアウト時間を設定します。

undo probe timeout コマンドはデフォルトに戻します。

プローブの時間以内にテストが完了しない場合、プローブがタイムアウトします。

このコマンドを有効にするには、**frequency** コマンドで指定した間隔が、このコマンドで指定した間隔よりも大きい必要があります。

例

DHCP テストのプローブタイムアウト時間を 10000 ミリ秒に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type dhcp

[AP-nqa-admin-test-dhcp] probe timeout 10000

HTTP テンプレートビューで、HTTP 操作のプローブタイムアウト時間を 10000 ミリ秒に設定します。

<AP> system-view

[AP] nqa template http httptplt

[AP-nqatplt-http-httptplt] probe timeout 10000

2.1.27

2.1.28 reaction checked-element probe-fail (for trap)

Syntax

reaction *item-number* **checked-element probe-fail threshold-type** { **accumulate** *accumulate-occurrences* | **consecutive** *consecutive-occurrences* } [**action-type** { **none** | **trap-only** }]

undo reaction *item-number*

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

ARP/DHCP/DLSw/DNS/FTP/HTTP operation view

定義済みユーザロール

network-admin

パラメータ

item-number: reaction entry に ID を割り当てます。設定範囲は 1～10 です。

threshold-type: しきい値タイプを指定します。

accumulate *accumulate-occurrences*: プローブが失敗する総数を確認します。設定範囲は 1～15 です。

consecutive *consecutive-occurrences*: 連続してテストに失敗する最大数を指定します。設定範囲は 1～16 です。

action-type: トリガーとなるアクションを指定します。デフォルトのアクションは **none** です。

none: ターミナル端末に結果を表示します。

trap-only: ターミナル端末に結果を表示し、NMS に SNMP トラップメッセージを送信します。DNS テストでは無効です。

説明

reaction checked-element probe-fail コマンドはテストのプローブの失敗をモニタするための reaction entry を設定します。

undo reaction コマンドは指定された reaction entry を削除します。

reaction を作成した後、修正することはできません。reaction entry の属性を変更する場合、**undo reaction** コマンドを使用して最初にエントリを削除し、新しい reaction entry を再度設定してください。

例

ICMP エコーテストのプローブ失敗をモニタするため、reaction entry 1 を作成します。NQA テストを開始する前に、reaction entry の初期状態は無効です。プローブが失敗した回数が 10 以上になった場合、エントリの状態をしきい値超過に設定します。しきい値が下回った場合、エントリの状態をしきい値以下に設定します。一度 reaction entry の状態が変更するとトラップメッセージを作成し、NMS に送信します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type accumulate 10 action-type trap-only

ICMP エコーテストのプローブ失敗をモニタするため、reaction entry 2 を作成します。NQA テストを開始する前に、reaction entry の初期状態は無効です。連続してプローブが失敗した回数が 10 以上になった場合、エントリの状態をしきい値超過に設定します。しきい値が下回った場合､エントリの状態をしきい値以下に設定します｡一度 reaction entry の状態が変更するとトラップメッセージを作成し、NMS に送信します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] reaction 2 checked-element probe-fail threshold-type consecutive 10 action-type trap-only

2.1.29 reaction trap

Syntax

reaction trap { **path-change** | **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** [*accumulate-probe-failures*] }

undo reaction trap { **probe-failure** | **test-complete** | **test-failure** }

デフォルト

設定なし

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

ICMP jitter/UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

path-change: **UDP tracert** 操作が宛先への別のパスを検出したときにトラップを送信します。

probe-failure *consecutive-probe-failures*: 連続してテストが失敗した後、NMS にトラップを送信するよう設定します。*consecutive-probe-failures* はテストにおける連続失敗数を設定します。設定範囲は 1～15 です。システムは複数のトラップを送信できるように各テストで連続して失敗した回数をカウントします。

test-complete: テストが完了したことを通知するためにトラップを送信します。

test-failure *accumulate-probe-failures*: プローブの失敗回数の総数が *accumulate-probe-failures* 以上になった場合、トラップを送信します。設定範囲は 1～15 です。システムは、1 つのトラップのみ送信するため、最後にテストを完了した後、プローブが失敗した総数をカウントします。

説明

reaction trap コマンドは指定した状況下で NMS にトラップを送信するように設定します。

undo reaction trap コマンドはデフォルトに戻します。

ICMP ジッタ、UDP ジッタ、および音声操作は、**test-complete** パラメータのみをサポートします。

次のパラメータは、**UDP tracert** 操作では使用できません。

- **probe-failure** *consecutive-probe-failures* オプション
- *accumulate-probe-failures* argument 引数

例

ICMP エコーテストで連続して 5 回以上失敗した場合、トラップを送信するように設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] reaction trap probe-failure 5

2.1.30 resolve-target

Syntax

resolve-target *domain-name*

undo resolve-target

デフォルト

設定なし

View

DNS operation view

DNS template view

定義済みユーザロール

network-admin

パラメータ

domain-name: 解決されるドメイン名を指定します。設定範囲は 1～255 文字です。ドットで区切り、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます（たとえば、aabbcc.com です）。各部分の設定範囲は 1～63 文字です。連続したドット（.）は使用できません。

説明

resolve-target コマンドは DNS テストのドメイン名を設定します。

undo resolve-target コマンドはデフォルトに戻します。

例

解決されるドメイン名 **domain1** を設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type dns

[AP-nqa-admin-test-dns] resolve-target domain1

DNS テンプレートビューで、解決するドメイン名として domain 1 を指定します。

<AP> system-view

[AP] nqa template dns dnstplt

[APe-nqatplt-dns-dnstplt] resolve-target domain1

2.1.31 route-option bypass-route

Syntax

route-option bypass-route

undo route-option bypass-route

デフォルト

無効

View

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

ICMP jitter/UDP jitter/voice operation view

定義済みユーザロール

network-admin

説明

route-option bypass-route コマンドはダイレクトな宛先への接続性を確認するため、ルーティングテーブルバイパス機能を有効にします。

undo route-option bypass-route コマンドはルーティングバイパス機能を無効にします。

ルーティングテーブルバイパス機能が有効であるとき、以下のイベントが発生します。

- ルーティングテーブルは検索されません。パケットはダイレクトに接続されたネットワークの宛先に直接送信されます。
- テストパケットの TTL が 1 に設定されます。**ttl** コマンドで設定された値は適用されません。

例

ルーティングテーブルバイパス機能を有効にします。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] route-option bypass-route

2.1.32 source interface (ICMP echo operation view/UDP tracert operation view)

Syntax

source interface *interface-type interface-number*

undo source interface

デフォルト

ICMP エコー要求パケットは送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

ICMP echo operation view

UDP tracert operation view

ICMP/tracert template view

定義済みユーザロール

network-admin

パラメータ

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

source interface コマンドは ICMP エコー要求パケットの送信元 IP アドレスとして指定したインタフェースの IP アドレスを指定します。

undo source interface コマンドはデフォルトに戻します。

指定したインタフェースはアップ状態にする必要があります。インタフェースがダウンしている場合、ICMP エコー要求は送信することができません。

source ip コマンドと **source interface** コマンドの両方を設定した場合、最後に行った設定が適用されます。

例

ICMP エコー要求パケットの送信元 IP アドレスとして VLAN インタフェース 2 の IP アドレスを設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] source interface vlan-interface 2

関連コマンド

source ip

2.1.33 source ip

Syntax

source ip *ip-address*

undo source ip

デフォルト

ICMP エコー要求パケットは送信元 IP アドレスとして送信インタフェースのプライマリ IP アドレスを使用します。

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

Any NQA template view

定義済みユーザロール

network-admin

パラメータ

ip-address: プローブパケットの送信元 IP アドレスを指定します。

説明

source ip コマンドはプローブパケットの送信元 IP アドレスを設定します。

undo source ip コマンドは指定された送信元アドレスを削除します。

指定された送信元 IP アドレスはローカルインタフェースの IP アドレスで、インタフェースがアップである必要があります。そうでなければプローブパケットは送信できません。

NQA テンプレートの場合､送信元アドレスと宛先アドレスの IP バージョンが異なると、送信元アドレスは有効になりません。

次の種類の NQA テストまたはテンプレートに対して **source interface** コマンドおよび **source ip** コマンドを複数回実行すると、最新の設定が有効になります。

- CMP エコーオペレーション.
- UDP tracert オペレーション
- ICMP テンプレート

例

ICMP エコー要求の送信元 IP アドレスを 10.1.1.1 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] source ip 10.1.1.1

関連コマンド

source interface

2.1.34 source port

Syntax

source port *port-number*

undo source port

デフォルト

設定なし

View

UDP echo operation view

SNMP operation view

UDP jitter/voice operation view

DNS/tracert template view

定義済みユーザロール

network-admin

パラメータ

port-number: 送信元ポート番号を指定します。設定範囲は 1～65535 です。

説明

source port コマンドはプローブパケットの送信元ポートを設定します。

undo source port コマンドは設定された送信元ポートを削除します。

例

UDP エコーテストのプローブパケットで送信元ポートを 8000 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type udp-echo

[AP-nqa-admin-test-udp-echo] source port 8000

2.1.35 statistics hold-time

Syntax

statistics hold-time *hold-time*

undo statistics hold-time

デフォルト

120 分

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

ICMP jitter/path jitter/UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

hold-time: 保持時間を指定します。設定範囲は 1～1440 分です。

説明

statistics hold-time コマンドは NQA テストの統計情報グループの保持時間を設定します。

undo statistics hold-time コマンドはデフォルトに戻します。

保持時間が終了したとき、統計情報グループは削除されます。

例

ICMP エコーテストの統計情報グループの保持時間を 3 分に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] statistics hold-time 3

2.1.36 statistics interval

Syntax

statistics interval *interval*

undo statistics interval

デフォルト

60 分

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

interval: 統計情報を収集する間隔を指定します。設定範囲は 1～35791394 分です。

説明

statistics interval コマンドは NQA テストで統計情報を収集する間隔を設定します。

undo statistics interval コマンドはデフォルトに戻します。

NQA は指定した間隔で NQA テストを行い、テスト結果の統計情報を計算します。これらの統計情報は統計情報グループを作ります。統計情報グループの情報を表示する場合、**display nqa statistics** コマンドを使用します。

例

ICMP エコーテストで統計情報を収集する間隔を 2 分に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] statistics interval 2

2.1.37 statistics max-group

Syntax

statistics max-group *number*

undo statistics max-group

デフォルト

2

View

ICMP echo/TCP/UDP echo operation view

DHCP/DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

定義済みユーザロール

network-admin

パラメータ

number: 統計情報グループの最大数を指定します。設定範囲は 0～100 です。統計情報の収集を無効にする場合、0 に設定します。

説明

statistics max-group コマンドは保存できる統計情報グループの最大数を設定します。

undo statistics max-group コマンドはデフォルトに戻します。

統計情報グループの数が最大数に到達し、新しいグループが保存されたとき、もっとも古い統計情報が削除されます。

例

ICMP エコーテストで保存できる統計情報グループの最大数を 5 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] statistics max-group 5

2.1.38 tos

Syntax

tos *value*

undo tos

デフォルト

0

View

すべての operation view

DNS/FTP/HTTP/HTTPS/ICMP/IMAP/POP3/RADIUS authentication/RADIUS accounting/RTSP/SIP/SMTP/SSL/TCP/TCP half open/UDP/WAP/tracert template view

定義済みユーザロール

network-admin

パラメータ

value: ToS を指定します。設定範囲は 0～255 です。

説明

tos コマンドはプローブパケットの IP ヘッダの ToS を設定します。

undo tos コマンドはデフォルトに戻します。

例

ICMP エコーテストでプローブパケットの IP ヘッダの ToS を 1 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] tos 1

#ICMP テンプレートビューで、プローブパケットの IP ヘッダの ToS 値を 1 に設定します。

<AP> system-view

[AP] nqa template icmp icmptplt

[AP-nqatplt-icmp-icmptplt] tos 1

2.1.39 ttl

Syntax

ttl *value*

undo ttl

デフォルト

20

View

ICMP echo/TCP/UDP echo operation view

DLSw/DNS/FTP/HTTP/SNMP operation view

UDP jitter/voice operation view

ICMP jitter/UDP jitter/voice operation view

DNS/FTP/HTTP/HTTPS/ICMP/IMAP/POP3/RADIUS authentication/RADIUS

accounting/RTSP/SIP/SMTP/SSL/TCP/TCP half open/UDP/WAP/tracert template view

定義済みユーザロール

network-admin

パラメータ

value: プローブパケットの TTL を指定します。設定範囲は 1～255 です。

説明

ttl コマンドはプローブパケットの TTL を指定します。

undo ttl コマンドはデフォルトに戻します。

route-option bypass-route コマンドはプローブパケットの TTL を 1 に設定します。**route-option bypass-route** コマンドと **ttl** コマンドを同時に実行した場合、**ttl** コマンドは適用されません。

UDP tracert テストをパスするには、指定された TTL 値が **init-ttl** コマンドで設定された値より小さくないことを確認します。

例

ICMP エコーテストでプローブパケットの TTL を 16 に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type icmp-echo

[AP-nqa-admin-test-icmp-echo] ttl 16

#ICMP テンプレートビューで、プローブパケットの最大ホップ数を 16 に設定します。

<AP> system-view

[AP] nqa template icmp icmptplt

[AP-nqatplt-icmp-icmptplt] ttl 16

2.1.40 type

Syntax

type { **arp** | **dhcp** | **dlsw** | **dns** | **ftp** | **http** | **icmp-echo** | **icmp-jitter** | **path-jitter** | **tcp** | **udp-echo** | **udp-jitter** | **udp-tracert** | **voice** }

デフォルト

設定なし

View

NQA operation view

定義済みユーザロール

network-admin

パラメータ

arp: ARP 動作タイプを指定します。

dhcp: DHCP テストタイプを指定します。

dlsw: DLSw テストタイプを指定します。

dns: DNS テストタイプを指定します。

ftp: FTP テストタイプを指定します。

http: HTTP テストタイプを指定します。

icmp-echo: ICMP エコーテストタイプを指定します。

icmp-jitter: ICMP ジッタ動作タイプを指定します。

path-jitter: パスジッタ動作タイプを指定します。

tcp: TCP テストタイプを指定します。

udp-echo: UDP エコーテストタイプを指定します。

udp-jitter: UDP ジッタテストタイプを指定します。

udp-tracert: UDP tracert 動作タイプを指定します。

voice: 音声テストタイプを指定します。

説明

type コマンドは NQA テストのテストタイプを設定し、operation type view に移行します。

NQA 操作に指定できるタイプは 1 つだけです。その後、NQA 操作の操作タイプ関連の設定を構成できます。NQA 操作のタイプを変更するには、システムビューで NQA 操作を削除してから、NQA 操作を再作成します。

例

FTP テストのテストタイプを設定し、FTP operation view に移行します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type ftp

[AP-nqa-admin-test-ftp]

2.1.41 url

Syntax

url *url*

undo url

デフォルト

設定なし

View

FTP/HTTP operation view

ICMP echo operation view

UDP jitter operation view

FTP/HTTP/HTTPS/RTSP/WAP/ICMP/TCP template view

定義済みユーザロール

network-admin

パラメータ

url: 宛先サーバの URL を指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。スペース、クエスチョンマーク（?）は使用できません。以下の表に異なるテストの URL のフォーマットとパラメータを示します。

テスト	URL フォーマット	デフォルトポート番号	パラメータの説明
HTTPテスト	*http://host/resource* *http://host:port/resource*	80	hostパラメータの設定範囲は1～255文字です。ドットで区切られ、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます。たとえばaabbcc.comです。各部分の設定範囲は1～63文字です。連続してドット（.）を設定することができません。ファイル名のパラメータの詳細は、オペレーションマニュアルのセクション1*基本機能“ファイルシステム管理”*を参照してください。
HTTPS テスト	https://host/resource https://host:port/resource	443	
FTPテスト	*ftp://host/filename* *ftp://host:port/filename*	21	

テスト	URL フォーマット	デフォルトポート番号	パラメータの説明
ICMPエコーテスト	protocol://host:port The host paramter is required. The protocol and port parameters can be unspecified or any values.	ー	hostパラメータの設定範囲は1～255文字です。ドットで区切られ、大文字、小文字を区別します。英字、数字、ハイフン（-）、アンダーライン（_）を含むことができます。たとえばaabbcc.comです。各部分の設定範囲は1～63文字です。連続してドット（.）を設定することができません。ファイル名のパラメータの詳細は、オペレーションマニュアルのセクション1*基本機能“ファイルシステム管理”*を参照してください。
UDPジッタテスト	protocol://host:port The host and port parameters are required. The protocol parameter can be unspecified or any value.	ー	
RTSPテスト	rtsp://host/resource rtsp://host:port/resource	554	
WAP テスト	http://host/filename http://host:port /filename https://host/resource https://host:port/resource	ー	

URL の port パラメータは、指定されている場合、サービスを提供する宛先サーバのポート番号を表します。

WAP 操作で url コマンドを有効にするには、WAP テンプレートビューで **expect** { **data** | **hex-data** } コマンドを設定する必要があります。

ICMP エコーテストまたは ICMP テンプレートの場合、url コマンドと **destination ip** コマンドは相互に排他的です。

UDP ジッタテストまたは TCP テンプレートの場合、url コマンドは **destination ip** コマンドおよび **destination port** コマンドと相互に排他的です。

説明

url コマンドは宛先 HTTP サーバあるいは宛先 FTP サーバの URL を指定します。

undo url コマンドは URL を削除します。

例

HTTP テストの URL を **http://www.company.com/index.htm** に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type http

[AP-nqa-admin-test-http] url http://www.company.com/index.html

#HTTP テンプレートビューで、HTTP 操作がアクセスする URL を **http://www.company.com/index.html** として設定します。

<AP> system-view

[AP] nqa template http httptplt

[AP-nqatplt-http-httptplt] url http://www.company.com/index.html

2.1.42 username

Syntax

username *username*

undo username

デフォルト

設定なし

View

FTP/HTTP operation view

FTP/HTTP/HTTPS/IMAP/POP3/RADIUS authentication/RADIUS accounting template view

定義済みユーザロール

network-admin

パラメータ

username: ユーザ名を指定します。設定範囲は 1～32 文字です。

- FTP、HTTP、または HTTPS ユーザ名は、1 から 32 文字の文字列です。
- POP 3 または IMAP ユーザ名は、username@domain.com の形式の 1～40 文字の文字列です。
- RADIUS 認証またはアカウンティングのユーザ名は、1 から 253 文字の文字列です。

説明

username コマンドは FTP あるいは HTTP ログインのユーザ名を指定します。

undo username コマンドは設定を削除します。

例

FTP ログインのユーザ名を **administrator** に設定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type ftp

[AP-nqa-admin-test-ftp] username administrator

#FTP テンプレートビューで FTP ログインユーザ名を **administrator** に設定します。

< AP > system-view

[AP] nqa template ftp ftptplt

[AP-nqatplt-ftp-ftptplt] username administrator

関連コマンド

- **operation**
- **password**

2.1.43 version

Syntax

version { **v1.0** | **v1.1** }

undo version

デフォルト

1.0

View

HTTP operation view

HTTP/HTTPS template view

定義済みユーザロール

network-admin

パラメータ

v1.0: HTTP バージョン 1.0 を使用します。

v1.1: HTTP バージョン 1.1 を使用します。

説明

version コマンドは HTTP テストで使用する HTTP バージョンを指定します。

undo version コマンドはデフォルトに戻します。

例

HTTP テストで使用する HTTP バージョンを 1.1 に指定します。

<AP> system-view

[AP] nqa entry admin test

[AP-nqa-admin-test] type http

[AP-nqa-admin-test-http] version v1.1

2.2 NQAサーバ設定コマンド

⚠ **重要**：

UDP ジッタテスト、TCP テスト、UDP エコーテスト、音声テストを行うため、NQA サーバを設定します。

2.2.1 display nqa server

Syntax

display nqa server

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display nqa server コマンドは NQA サーバの状態を表示します。

例

NQA サーバの状態を表示します。

<AP> display nqa server

```
NQA server status: Enabled
TCP connect:
  IP Address         Port     ToS    VPN instance
  2.2.2.2           2000     200    -
UDP echo:
  IP Address         Port     ToS    VPN instance
  3.3.3.3           3000     255    -
```

表 2-7 コマンド出力

フィールド	説明
NQA server status	NQAサーバが有効かどうかを示します。
TCP connect	NQAサーバのTCPリスニングサービスの情報です。
UDP echo	NQAサーバのUDPリスニングサービスの情報です。
IP Address	NQAサーバのTCP/UDPリスニングサービスで指定されたIPアドレスです。
Port	NQAサーバのTCP/UDPリスニングサービスでの指定されたポート番号です。
ToS	NQAサーバが送信する応答パケットのToSの値です。
VPN instance	このフィールドは現在のソフトウェアバージョンでサポートしていません。

関連コマンド

- **nqa server enable**
- **nqa server tcp-connect**
- **nqa server udp-echo**

2.2.2 nqa server enable

Syntax

nqa server enable

undo nqa server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

nqa server enable コマンドは NQA サーバを有効にします。

undo nqa server enable コマンドは NQA サーバを無効にします。

例

NQA サーバを有効にします。

<AP> system-view

[AP] nqa server enable

関連コマンド

- **display nqa server**
- **nqa server tcp-connect**
- **nqa server udp-echo**

2.2.3 nqa server tcp-connect

Syntax

nqa server tcp-connect *ip-address port-number* [**tos** *tos*]

undo nqa server tcp-connect *ip-address port-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: TCP リスニングサービスの IP アドレスを指定します。

port-number: TCP リスニングサービスのポート番号を指定します。設定範囲は 1～65535 です。

tos *tos*: 応答パケットの IP ヘッダの ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

nqa server tcp-connect コマンドは NQA サーバが指定された IP アドレスとポート番号をリスニングし、応答するため、TCP リスニングサービスを設定します。

undo nqa server tcp-connect コマンドは TCP リスニングサービスを削除します。

このコマンドは NQA サーバ上で TCP テストのみに使用されます。

NQA サーバの TCP リスニングサービスの IP アドレスとポート番号を設定するとき、以下の制限とガイドラインに従ってください。

- IP アドレスとポート番号は NQA サーバで固有に設定し、NQA クライアントの設定に一致するようにしてください。
- IP アドレスは NQA サーバのインタフェースの IP アドレスにする必要があります。
- NQA テストを正常に実行し、既存のサービスへの影響を防ぐため、TCP リスニングサービスで 1～1023 の well-known ポートを設定しないでください。

例

NQA サーバで TCP リスニングサービスを設定します。IP アドレス 169.254.10.2、ポート番号 9000 をリスニングし、応答するように設定します。

<AP> system-view

[AP] nqa server tcp-connect 169.254.10.2 9000

関連コマンド

- **display nqa server**
- **nqa server enable**

2.2.4 nqa server udp-echo

Syntax

nqa server udp-echo *ip-address port-number* [**tos** *tos*]

undo nqa server udp-echo *ip-address port-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: UDP リスニングサービスの IP アドレスを指定します。

port-number: UDP リスニングサービスのポート番号を指定します。設定範囲は 1～65535 です。

tos *tos*: 応答パケットの IP ヘッダの ToS を指定します。設定範囲は 0～255 です。デフォルトは 0 です。

説明

nqa server udp-echo コマンドは NQA サーバが指定された IP アドレスとポート番号をリスニングし、応答するため、UDP リスニングサービスを設定します。

undo nqa server udp-echo コマンドは UDP リスニングサービスを削除します。

このコマンドは NQA サーバ上で UDP ジッタテスト、UDP エコーテスト、音声テストのみに使用されます。

NQA サーバの UDP リスニングサービスの IP アドレスとポート番号を設定するとき、以下の制限とガイドラインに従ってください。

- IP アドレスとポート番号は NQA サーバで固有に設定し、NQA クライアントの設定に一致するようにしてください。
- IP アドレスは NQA サーバのインタフェースの IP アドレスにする必要があります。
- NQA テストを正常に実行し、既存のサービスへの影響を防ぐため、UDP リスニングサービスで 1～1023 の well-known ポートを設定しないでください。

例

NQA サーバで UDP リスニングサービスを設定します。IP アドレス 169.254.10.2、ポート番号 9000 をリスニングし、応答するように設定します。

<AP> system-view

[AP] nqa server udp-echo 169.254.10.2 9000

関連コマンド

- **display nqa server**
- **nqa server enable**

目次

このセクションのページは **15-x-x** です。

3 章 SNMP 3-1
3.1 SNMP 設定コマンド 3-1
3.1.1 display snmp-agent community 3-1
3.1.2 display snmp-agent group 3-4
3.1.3 display snmp-agent local-engineid 3-6
3.1.4 display snmp-agent mib-view 3-7
3.1.5 display snmp-agent statistics 3-9
3.1.6 display snmp-agent sys-info 3-12
3.1.7 display snmp-agent trap queue 3-13
3.1.8 display snmp-agent trap-list 3-14
3.1.9 display snmp-agent usm-user 3-15
3.1.10 enable snmp trap updown 3-18
3.1.11 simulate snmp-trap 3-19
3.1.12 snmp-agent 3-21
3.1.13 snmp-agent calculate-password 3-23
3.1.14 snmp-agent community 3-25
3.1.15 snmp-agent group 3-28
3.1.16 snmp-agent local-engineid 3-31
3.1.17 snmp-agent log 3-33
3.1.18 snmp-agent mib-view 3-35
3.1.19 snmp-agent packet max-size 3-37
3.1.20 snmp-agent sys-info contact 3-38
3.1.21 snmp-agent sys-info location 3-39
3.1.22 snmp-agent sys-info version 3-40
3.1.23 snmp-agent target-host 3-41
3.1.24 snmp-agent trap enable 3-43
3.1.25 snmp-agent trap if-mib link extended 3-45
3.1.26 snmp-agent trap life 3-46
3.1.27 snmp-agent trap log 3-47
3.1.28 snmp-agent trap queue-size 3-48
3.1.29 snmp-agent usm-user { v1 | v2c } 3-49
3.1.30 snmp-agent usm-user v3 3-52

3章 SNMP

SNMP エージェントはリンク状態の変更、ユーザのログイン、ログアウトのような重要なイベントを NMS に知らせるため、notification（トラップと inform）を送信します。特に指定しない限り、コマンドラインの trap キーワードは trap と inform を含みます。

3.1 SNMP設定コマンド

3.1.1 display snmp-agent community

Syntax

display snmp-agent community [**read** | **write**]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

read: 読み出し専用コミュニティ情報を表示します。

write: 読み出し、書き込みコミュニティ情報を表示します。

説明

display snmp-agent community コマンドは SNMPv1 あるいは SNMPv2c のコミュニティ情報を表示します。

パラメータを指定しない場合、作成されたすべての SNMPv1 あるいは SNMPv2c のコミュニティ情報を表示します。

このコマンドは以下の方法で作成された SNMPv1、SNMPv2c コミュニティを表示します。

- **snmp-agent community** コマンドで作成されたコミュニティ
- 既存の SNMP グループに割り当てられた SNMPv1 と SNMPv2c のユーザ用に自動で作成されたコミュニティ

例

すべての SNMPv1 あるいは SNMPv2c のコミュニティ情報を表示します。

<AP> display snmp-agent community

```
   Community name: aa
      Group name: aa
      ACL:2001
      Storage-type: nonVolatile
      Context name: con1

   Community name: bb
      Role name: bb
      Storage-type: nonVolatile

   Community name: userv1
      Group name: testv1
      Storage type: nonvolatile
Community name: cc
      Group name: cc
      ACL name: testacl
      Storage type: nonVolatile
```

表 3-1 コマンド出力

フィールド	説明
Community name	**snmp-agent community**コマンドで作成されたコミュニティ名あるいは**snmp-agent usm-user** { **v1** | **v2c** }コマンドで作成されたユーザ名を表示します。
Group name	SNMPグループ名です。 ● **snmp-agent community**コミュニティがコマンドで作成された場合、グループ名はコミュニティ名と同一です。 ● **snmp-agent usm-user** { **v1** | **v2c** }コミュニティがコマンドで作成された場合、ユーザがあるグループ名が表示されます。
Role name	コミュニティのユーザロールです。 コミュニティがRBACモードの**snmp-agent community**コマンドで作成された場合、ユーザロールはコミュニティ名と結合できます。
ACL	ACL番号です。 このフィールドはSNMPv1あるいはSNMPv2cコミュニティで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	ACL名です。 このフィールドはSNMPv1あるいはSNMPv2cコミュニティで、ACL名が指定されたときのみ表示されます。ACLフィールドと一緒に表示されません。

フィールド	説明
Storage-type	記憶媒体のタイプです。 • **volatile**—システムが再起動したときに設定が失われます。 • **nonVolatile**—システムが再起動しても設定は失われません。 • **permanent**—システムが再起動しても設定は失われません。変更することができますが、削除することができません。 • **readOnly**—システムが再起動しても設定は失われません。変更あるいは削除することができません。 • **other**—他の記憶媒体のタイプです。
Context name	SNMPの内容です。 • SNMPコミュニティとSNMPの内容間のマッピングが設定されている場合、SNMPの内容が表示されます。 • SNMPコミュニティとSNMPの内容間のマッピングが設定されていない場合、表示されません。

関連コマンド

- **snmp-agent community**
- **snmp-agent usm-user { v1 | v2c }**

3.1.2 display snmp-agent group

Syntax

display snmp-agent group [*group-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-name: SNMPv1、SNMPv2c、SNMPv3 グループ名を指定します。設定範囲は 1～32 です。大文字、小文字を区別します。指定しない場合、すべての SNMP グループの情報を表示します。

説明

display snmp-agent group コマンドは SNMP グループの情報を表示します。

例

すべての SNMP グループの情報を表示します。

<AP> display snmp-agent group

```
  Group name: groupv3
     Security model: v3 noAuthnoPriv
     Readview: ViewDefault
     Writeview: <no specified>
     Notifyview: <no specified>
     Storage-type: nonvolatile
ACL name: testacl
```

表 3-2 コマンド出力

フィールド	説明
Group name	SNMPグループ名です。

フィールド	説明
Security model	SNMPグループのセキュリティモデルです。 ● **authPriv**—プライバシーセキュリティありの認証です。 ● **authNoPriv**—プライバシーセキュリティなしの認証です。 ● **noAuthNoPriv**—認証なし、プライバシーセキュリティなしです。 SNMPv1あるいはSNMPv2cグループのセキュリティモデルはnoAuthNoPrivのみです。
Readview	SNMPグループにアクセス可能な読み込み専用のMIB viewです。
Writeview	SNMPグループにアクセス可能な書き込みのMIB viewです。
Notifyview	SNMP viewの通知MIB viewです。グループのSNMPユーザは通知MIB viewのノードの通知を送信できます。
Storage-type	記憶媒体のタイプです。**volatile**、**nonvolatile**、**permanent**、**readOnly**、**other**が含まれます。（表 3-1を参照してください。）
ACL	ACL番号です。 このフィールドはSNMPグループで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	ACL名です。 このフィールドはSNMPグループで、ACL名が指定されたときのみ表示されます。ACLフィールドと一緒に表示されません。

関連コマンド

snmp-agent group

3.1.3 display snmp-agent local-engineid

Syntax

display snmp-agent local-engineid

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent local-engineid コマンドはローカル SNMP エンジン ID を表示します。

各 SNMP エージェントはメッセージの送受信、メッセージの認証、暗号化、管理されたオブジェクトへのアクセス制御のサービスを提供するため 1 つの SNMP エンジンがあります。

ローカル SNMP エンジン ID は SNMP ドメインの SNMP エージェントの SNMP エンジンを固有に識別します。

例

ローカル SNMP エンジン ID を表示します。

<AP> display snmp-agent local-engineid

```
SNMP local engine ID: 800063A2800084E52BED7900000001
```

関連コマンド

snmp-agent local-engineid

3.1.4 display snmp-agent mib-view

Syntax

display snmp-agent mib-view [**exclude** | **include** | **viewname** *view-name*]

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

exclude: MIB view から除外されたサブツリーを表示します。

include: MIB view から含まれるサブツリーを表示します。

viewname *view-name*: 指定された MIB view の情報を表示します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

説明

display snmp-agent mib-view コマンドは MIB view を表示します。

パラメータを指定しない場合、すべての MIB view を表示します。

例

すべての MIB view を表示します。

<AP> display snmp-agent mib-view

```
  View name: ViewDefault
     MIB Subtree: iso
     Subtree mask:
     Storage-type: nonVolatile
     View Type: included
     View status: active

  View name: ViewDefault
     MIB Subtree: snmpUsmMIB
     Subtree mask:
     Storage-type: nonVolatile
     View Type: excluded
     View status: active

  View name: ViewDefault
     MIB Subtree: snmpVacmMIB
```

```
    Subtree mask:
    Storage-type: nonVolatile
    View Type: excluded
    View status: active

View name: ViewDefault
    MIB Subtree: snmpModules.18
    Subtree mask:
    Storage-type: nonVolatile
    View Type: excluded
    View status: active
```

ViewDefault はデフォルトの MIB view です。出力は **snmpUsmMIB**、**snmpVacmMIB**、**snmpModules.18** の MIB オブジェクトを除いて **iso** サブツリーのすべての MIB オブジェクトがアクセス可能です。

表 3-3 コマンド出力

フィールド	説明
View name	MIB view名です。
MIB Subtree	MIB viewで扱われるMIBサブツリーです。
Subtree mask	MIBサブツリーマスクです。
Storage-type	サブツリーが記録される記憶媒体（表 3-1を参照してください）のタイプです。
View Type	MIB viewのMIBサブツリーのアクセス権です。 • **Included**—MIBサブツリーのすべてのオブジェクトがMIB viewにアクセス可能です。 • **Excluded**—MIBサブツリーのすべてのオブジェクトがMIB viewにアクセス可能できません。
View status	MIB viewの状態です。 • **active**—MIB viewが有効です。 • **inactive**—MIB viewは、CLIで作成されるとactiveになります。MIB viewを削除せずに一時的に無効にするには、SNMPセット操作を実行してステータスをinactiveに設定します。

関連コマンド

snmp-agent mib-view

3.1.5 display snmp-agent statistics

Syntax

display snmp-agent statistics

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent statistics コマンドは SNMP メッセージの統計情報を表示します。

例

SNMP メッセージの統計情報を表示します。

<AP> display snmp-agent statistics

```
1684 messages delivered to the SNMP entity.
5 messages were for an unsupported version.
0 messages used an unknown SNMP community name.
0 messages represented an illegal operation for the community supplied.
0 ASN.1 or BER errors in the process of decoding.
1679 messages passed from the SNMP entity.
0 SNMP PDUs had badValue error-status.
0 SNMP PDUs had genErr error-status.
0 SNMP PDUs had noSuchName error-status.
0 SNMP PDUs had tooBig error-status (Maximum packet size 1500).
16544 MIB objects retrieved successfully.
2 MIB objects altered successfully.
7 GetRequest-PDU accepted and processed.
7 GetNextRequest-PDU accepted and processed.
1653 GetBulkRequest-PDU accepted and processed.
1669 GetResponse-PDU accepted and processed.
2 SetRequest-PDU accepted and processed.
0 Trap PDUs accepted and processed.
0 alternate Response Class PDUs dropped silently.
0 forwarded Confirmed Class PDUs dropped silently.
```

表 3-4 コマンド出力

フィールド	説明
messages delivered to the SNMP entity	SNMPエージェントが受信したメッセージ数です。
messages were for an unsupported version	SNMPエージェントのバージョンでサポートされていないメッセージ数です。
messages used an unknown SNMP community name	不明なSNMPコミュニティ名が使用されたメッセージ数です。
messages represented an illegal operation for the community supplied	コミュニティを実行する権限がないオペレーションが運ばれたメッセージ数です。
ASN.1 or BER errors in the process of decoding	復号化の間にASN.1あるいはBERエラーがあるメッセージ数です。
messages passed from the SNMP entity	SNMPエージェントによって送信されたメッセージ数です。
SNMP PDUs had badValue error-status	BadValueエラーのPDU数です。
SNMP PDUs had genErr error-status	genErrエラーのPDU数です。
SNMP PDUs had noSuchName error-status	NoSuchNameエラーのPDU数です。
SNMP PDUs had tooBig error-status	TooBigエラーのPDU数です。（最大パケットサイズが1500バイトです）
MIB objects retrieved successfully	正常に読み込まれたMIBオブジェクト数です。
MIB objects altered successfully	正常に書き込まれたMIBオブジェクト数です。
GetRequest-PDU accepted and processed	読み込み、処理されたGetRequest要求の数です。
GetNextRequest-PDU accepted and processed	読み込み、処理されたgetNext要求の数です。
GetBulkRequest-PDU accepted and processed	読み込み、処理されたgetBulk要求の数です。
GetResponse-PDU accepted and processed	読み込み、処理されたget応答の数です。
SetRequest-PDU accepted and processed	読み込み、処理されたset要求の数です。
Trap PDUs accepted and processed	読み込み、処理された通知の数です。
alternate Response Class PDUs dropped silently	廃棄された応答パケットの数です。

フィールド	説明
forwarded Confirmed Class PDUs dropped silently	廃棄された転送パケットの数です。

3.1.6 display snmp-agent sys-info

Syntax

display snmp-agent sys-info [**contact** | **location** | **version**] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

contact: システム連絡先を表示します。

location: 装置の所在地を表示します。

version: SNMP エージェントのバージョンを表示します。

説明

display snmp-agent sys-info コマンドは SNMP エージェントシステムの情報を表示します。

パラメータを指定しない場合、すべての SNMP エージェントシステムの情報を表示します。

例

すべての SNMP エージェントシステムの情報を表示します。

<AP> display snmp-agent sys-info

```
The contact information of the agent:

The location information of the agent:

The SNMP version of the agent:
   SNMPv3
```

関連コマンド

snmp-agent sys-info

3.1.7 display snmp-agent trap queue

Syntax

display snmp-agent trap queue

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent trap queue コマンドは trap キューの基本情報を表示します。

例

trap キューの設定と使用状態を表示します。

<AP> display snmp-agent trap queue

```
Queue size: 100
Message number: 6
```

関連コマンド

- **snmp-agent trap life**
- **snmp-agent trap queue-size**

3.1.8 display snmp-agent trap-list

Syntax

display snmp-agent trap-list

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display snmp-agent trap-list コマンドは SNMP 通知（notification）を作成できるモジュールの SNMP 通知機能の状態（**enable** あるいは **disable**）を表示します。

モジュールのサブモジュールで、サブモジュールで SNMP 通知機能が有効である場合、SNMP 通知機能が有効であることを表示します。

モジュールで SNMP 通知機能をサポートしているかどうか確認する場合、**snmp-agent trap enable ?**コマンドを使用します。

display snmp-agent trap-list コマンドの出力は **snmp-agent trap enable** コマンドの設定とモジュールの設定によって異なります。

例

モジュールの SNMP 通知機能の状態を表示します。

<AP> display snmp-agent trap-list

```
arp notification is disabled.
configuration notification is enabled.
mac-address notification is enabled.
radius notification is disabled.
standard notification is enabled.
syslog notification is disabled.
system notification is enabled.

Enabled notifications: 4; Disabled notifications: 3
```

関連コマンド

snmp-agent trap enable

3.1.9 display snmp-agent usm-user

Syntax

display snmp-agent usm-user [**engineid** *engineid* | **group** *group-name* | **username** *user-name*] *

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

engineid *engineid*: SNMP エンジン ID の SNMPv3 ユーザ情報を表示します。SNMP エンジン ID は *engineid* で識別されます。*engineid* は大文字、小文字を区別しません。SNMPv3 ユーザが作成されているとき、システムはローカル SNMP エンティティのエンジン ID を記録します。エンジン ID が変更されるとユーザは無効になり、記録されたエンジン ID が復元されるとユーザが有効になります。

group *group-name*: 指定した SNMP グループ名の SNMPv3 ユーザ情報を表示します。グループ名は大文字、小文字を区別します。

username *user-name*: 指定した SNMPv3 ユーザの情報を表示します。ユーザ名は大文字、小文字を区別します。

説明

display snmp-agent usm-user コマンドは SNMPv3 ユーザ情報を表示します。

このコマンドは **snmp-agent usm-user v3** コマンドを使用して作成された SNMPv3 ユーザのみ表示します。**snmp-agent usm-user** { **v1** | **v2c** }コマンドを使用して作成された SNMPv1 あるいは SNMPv2c ユーザを表示する場合、**display snmp-agent community** コマンドを使用します。

例

すべての SNMPv3 ユーザ情報を表示します。

<AP> display snmp-agent usm-user

```
Username: userv3
Group name: mygroupv3
   Engine ID: 800063A203000FE240A1A6
   Storage-type: nonVolatile
   UserStatus: active
   ACL: 2000
```

```
Username: userv3
Group name: mygroupv3
    Engine ID: 8000259503000BB3100A508
    Storage type: nonVolatile
    User Status: active
    ACL name: testacl

Username: userv3code
Role name: groupv3code
          network-operator
    Engine ID: 800063A203000FE240A1A6
    Storage type: nonVolatile
    User Status: active

Username: userv3code
Role name: snmprole
          network-operator
    Engine ID: 800063A280000002BB0001
    Storage type: nonVolatile
    User Status: active
```

表 3-5 コマンド出力

フィールド	説明
Username	SNMPユーザ名です。
Group name	SNMPグループ名です。
Role name	SNMPユーザロール名です。
Engine ID	SNMPユーザが作成されたとき、SNMPエージェントが使用したエンジンIDです。
Storage-type	記憶媒体のタイプです。 • **volatile** • **nonVolatile** • **permanent** • **readOnly** • **other** 記憶媒体の詳細は表 3-1を参照してください。

フィールド	説明
UserStatus	SNMPユーザの状態です。 ● **active**—SNMPユーザは動作しています。 ● **notInService**—SNMPユーザは正常に設定されていますが、動作していません。 ● **notReady**—SNMPユーザの設定が不完全です。 ● **other**—他の状態です。
ACL	ACL番号です。 このフィールドはSNMPv3ユーザで、ACLが指定されたときのみ表示されます。ACL名フィールドと一緒に表示されません。
ACL name	ACL名です。 このフィールドはSNMPv3ユーザで、ACL名が指定されたときのみ表示されます。ACLフィールドと一緒に表示されません。

関連コマンド

snmp-agent usm-user v3

3.1.10 enable snmp trap updown

Syntax

enable snmp trap updown

undo enable snmp trap updown

デフォルト

有効

View

Interface view

定義済みユーザロール

network-admin

説明

enable snmp trap updown コマンドはインタフェースのリンク状態の通知を有効にします。

undo enable snmp trap updown コマンドはインタフェースのリンク状態の通知を無効にします。

状態が変更したとき、インタフェースで linkUp/linkDown の通知を作成する場合、**snmp-agent trap enable standard** [**linkdown** | **linkup**] *コマンドを使用してグローバルに linkUp/linkDown 通知機能を有効にする必要があります。

例

GigabitEthernet 1/0/1 で linkUp/linkDown の SNMP trap を 10.1.1.1 に送信することを有効にします。コミュニティ名は **public** を使用します。

<AP> system-view

[AP] snmp-agent trap enable

[AP] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public

[AP] interface gigabitethernet 1/0/1

[AP-GigabitEthernet1/0/1] enable snmp trap updown

関連コマンド

- **snmp-agent target-host**
- **snmp-agent trap enable**

3.1.11 simulate snmp-trap

Syntax

simulate snmp-trap all [**ifindex** *ifindex*]

simulate snmp-trap trap-node *name-string* [**context** *context-name*] [**variable-binding** { *variable-binding-name* { **hex** *hex-value* | **null-string** | *variable-binding-value* } } &<1-n>]

View

System view

定義済みユーザロール

network-admin

パラメータ

all：すべての SNMP 通知を指定します。

ifindex *ifindex*: SNMP 通知で送信される ifindex バインド（ノードとも呼ばれます）の値を指定します。値は、装置に存在する任意のインタフェースのインデックスにすることができます。このパラメータを指定しない場合、既存のインタフェースのインデックスを自動的に選択します。

trap-node *name-string*: SNMP 通知ノードを名称もしくは OID で指定します。このパラメータは大文字と小文字を区別しません。1～255 文字で既存のノードを指定してください。

context *context-name*: SNMP コンテキストを指定します。大文字と小文字を区別します。1～32 文字で指定してください。いくつかの通知ノードは異なるシナリオで使用できます。このパラメータは通知が引き起こされる特定のシナリオを示すために使用されます。

variable-binding { *variable-binding-name* { **hex** *hex-value* | **null-string** | *variable-binding-value* } } &<1-n> : SNMP 通知で送信される多様なバインドを指定します。

- *variable-binding-name*: 変数名もしくは OID を指定します。大文字と小文字は区別せず、通知ノードにサポートされる必要があります。
- **hex** *hex-value*: 16 進数形式で指定します。大文字と小文字は区別しません。1～255 の 16 進数で指定します。値は偶数にする必要があります。ベストプラクティスとして、16 進数以外の文字列として変数の値を設定します。ただし、変数値に文字列として直接表現できない特殊文字が含まれている場合は、値を 16 進数形式で設定します。変数バインド値を 16 進数形式で設定する場合は、最初に文字を ASCII コードに変換してから、ASCII コードを 16 進値に変換してください。
- **null-string**: 変数のバインドがヌル文字列であることを示します。
- *variable-binding-value*: 変数を 16 進数ではない形式で指定します。大文字と小文字を区別しません。1 から 255 の 16 進数文字ではない文字列です。
- &<1-n>: 最大 n 個の変数バインドを指定できることを示します。n の値は、通知ノードによって異なります。

説明

simulate snmp-trap コマンドは SNMP 通知送信をシミュレートします。

1) アプリケーションシナリオ
この機能は SNMP 通知機能が正常かどうか、通知設定が正しいか、NMS が通知を受信し正常に解析できるかどうかをテストできます。NMS が SNMP 通知を受信できない場合、問題を特定し、解決するためのトラブルシューティングを実施します。
2) 動作メカニズム
この機能を設定すると、装置は各ノードのメッセージを含む SNMP 通知を生成し、生成した通知を SNMP モジュールから送信します。
生成された SNMP 通知で送信されるノードは、以下のような値が割り当てられます。

- **数字タイプノード**—ノードの範囲の最小値を指定します。値の範囲がないノードには、0 が割り当てられます。
- **文字タイプノード**—値は Test です。文字数の指定要件がある場合、要件を満たすまで“Test”を切り捨てるか、繰り返します。
- **タイムスタンプタイプノード**—現在のシステム時刻を指定します。
- **IPv4 アドレスタイプノード**—“127.0.0.1”を指定します。
- **ビットタイプノード**—ノードのデフォルト値を使用します。デフォルト値がないノードの場合、ノードの設定範囲の最小値を使用します。
- **パスワードタイプノード**—値は“******”です。
- **オブジェクト識別子ノード**—値は通知の OID です。

同じイベントの通知とリカバリ通知は順番に送信されます。
通知ノードに同じ名前の変数が複数含まれている場合、同一の変数と値を順番に指定してください。変数に値を指定しない場合、上記の規則に基づいて値が割り当てられます。

この機能を有効にする前に、SNMP を有効にする必要があります。また、通知が送信されるようにするために、**snmp-agent target-host** コマンドを実行し、SNMP 通知のターゲットホストを指定してください。必要に応じて別の SNMP パラメータを設定してください。

このコマンドを設定するためのヘルプ情報を取得するには、コマンドの特定のパラメーター位置に「?」を入力します。たとえば、デバイスでサポートされているトラップ通知を取得するには、simulate snmp-trap trap-node ? のようにコマンドに「?」と入力します。

メモ

このコマンドは QX-W610 v7.5.114 を含む以降のバージョンからサポートしています。

例

サポートされているすべての SNMP 通知の送信をシミュレートします。

<AC> system-view

[AC] simulate snmp-trap all

```
This operation will take long time and is resources-intensive. Continue?[Y/N]:y
```

関連コマンド

- **snmp-agent**
- **snmp-agent target-host**

3.1.12 snmp-agent

Syntax

snmp-agent

undo snmp-agent

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent コマンドは SNMP エージェントを有効にします。

undo snmp-agent コマンドは SNMP エージェントを無効にします。

snmp-agent calculate-password を除く **snmp-agent** で始まるコマンドを実行するとき、SNMP エージェントは自動で有効になります。

🕮 **メモ：**

- デフォルトコンフィグが設定された装置で **snmp-agent** コマンドを設定すると、**snmp-agent local-engineid** コマンドと **snmp-agent sys-info version v3** コマンドが自動的に追加されます。
- snmp の設定を変更した装置を **undo snmp-agent** コマンドによって無効した後、再度 snmp を有効にすると **undo** コマンド実行前の設定状態に戻ります。

例

SNMP エージェントを有効にします。

<AP> system-view

[AP] snmp-agent

3.1.13 snmp-agent calculate-password

Syntax

snmp-agent calculate-password *plain-password* **mode** { **3desmd5** | **3dessha** | **md5** | **sha** } { **local-engineid** | **specified-engineid** *engineid* }

View

System view

定義済みユーザロール

network-admin

パラメータ

plain-password: プレーンテキストの認証あるいはプライバシーキーを指定します。設定範囲は 1～64 文字です。大文字、小文字を区別します。

mode:認証アルゴリズムと暗号化アルゴリズムを指定します。装置は、HMAC-MD5、HMAC-SHA1 認証アルゴリズムをサポートします。HMAC-MD5 は HMAC-SHA1 よりも計算が早いですが、HMAC-SHA1 は HMAC-MD5 よりもセキュリティ強度が高いです。

暗号化アルゴリズムは AES、3DES、DES の順番でセキュリティ強度が弱くなります。セキュリティ強度が強いアルゴリズムは計算が遅くなります。DES は一般的なセキュリティの要件を満たすのに十分です。

- **3desmd5**: HMAC-MD5 認証アルゴリズムと連携して使用される 3DES 認証キーのため、プライバシーキーをプレーンテキストから暗号テキストに変換します。
- **3dessha**: HMAC-SHA1 認証アルゴリズムと連携して使用される 3DES 認証キーのため、プライバシーキーをプレーンテキストから暗号テキストに変換します。
- **md5**: HMAC-SHA1 認証アルゴリズムと AES あるいは DES 暗号化アルゴリズムを使用して認証キーあるいは暗号化キーをプレーンテキストから暗号テキストに変換します。HMAC-MD5 認証アルゴリズムが使用されるとき、AES あるいは DES 暗号化アルゴリズムが使用されているかどうかにかかわらず、同一の認証キーあるいは暗号化キーを使用します。
- **sha**: HMAC-SHA1 認証アルゴリズムと AES あるいは DES 暗号化アルゴリズムを使用して認証キーあるいは暗号化キーをプレーンテキストから暗号テキストに変換します。HMAC-SHA1 認証アルゴリズムが使用されるとき、AES あるいは DES 暗号化アルゴリズムが使用されているかどうかにかかわらず、同一の認証キーあるいは暗号化キーを使用します。

local-engineid: 暗号テキストのキーを計算するためローカルエンジン ID を使用します。**snmp-agent local-engineid** コマンドでローカルエンジン ID を設定することができます。

specified-engineid *engineid*: 暗号テキストのキーを計算するためユーザ定義のエンジン ID を使用します。*engineid* は 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。

説明

snmp-agent calculate-password コマンドは暗号テキストの認証あるいは SNMPv3 でプレーンテキストから変換されたプライバシーキーのダイジェストを計算します。

snmp-agent calculate-password コマンドを実行する前に SNMP エージェントが有効であることを確認してください。

セキュリティのため、**snmp-agent usm-user v3** コマンドを使用して SNMPv3 ユーザを作成するとき、暗号テキストの認証とプライバシーキーのダイジェストを計算するために、**snmp-agent calculate-password** コマンドを使用します。

変換されたキーは変換のため、指定されたエンジン ID でのみ有効です。

例

プレーンテキスト **authkey** から変換された暗号テキストのダイジェストを計算するため、ローカルエンジンと HMAC-SHA1 アルゴリズムを使用します。

<AP> system-view

[AP] snmp-agent calculate-password authkey mode sha local-engineid

```
The encrypted key is: 09659EC5A9AE91BA189E5845E1DDE0CC
```

関連コマンド

- **snmp-agent local-engineid**
- **snmp-agent usm-user v3**

3.1.14 snmp-agent community

Syntax

snmp-agent community { **read** | **write** } [**simple** | **cipher**] *community-name* [**mib-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent community [**cipher**] *community-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

read: 指定されたコミュニティを MIB オブジェクトへの読み出し専用のアクセス権限に割り当てます。読み出し専用コミュニティは MIB 情報を問い合わせることのみ可能です。

write: 指定されたコミュニティを MIB オブジェクトへの読み出し、書き込みのアクセス権限に割り当てます。読み出し専用コミュニティは MIB 情報を設定することができます。

simple: プレーンテキストのコミュニティを設定します。セキュリティのため、コミュニティは暗号テキストで保存されます。

cipher: 暗号テキストのコミュニティを設定し、暗号テキストで保存します。

community-name: コミュニティを設定します。大文字、小文字を区別します。プレーンテキストの設定範囲は 1～32 文字です。暗号テキストの設定範囲は 33～73 文字です。バックスラッシュの後にエスケープ文字として文字列を入力します。

mib-view *view-name*: コミュニティで有効な MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。MIB view はアクセス可能な MIB オブジェクトの一式を示します。MIB view を指定しない場合、コミュニティはデフォルト MIB view の **ViewDefault** の MIB オブジェクトにアクセスできます。

acl: 標準 IPv4 ACL コミュニティを指定します。

ipv4-acl-number: 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 IPv4 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

snmp-agent community コマンドは SNMPv1 あるいは SNMPv2c コミュニティを設定します。

undo snmp-agent community コマンドは SNMPv1 あるいは SNMPv2c コミュニティを削除します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMP コミュニティは NMS と SNMP エージェントの一式を構成し、コミュニティによって識別します。NMS と SNMP エージェントは互いにに称するため、同じコミュニティを使用する必要があります。

通常、**public** は読み込み専用のコミュニティとして使用され、**private** は読み込み、書き込みコミュニティとして使用します。セキュリティを改善するため、SNMP コミュニティに **public** と **private** 以外の名前を割り当てます。

SNMP コミュニティで MIB オブジェクトにアクセスを制御するため、以下のモードを使用することができます。

- **VACM（View ベースアクセス制御モデル）**—VACM モードは MIB view を SNMP コミュニティに割り当てることで MIB オブジェクトへのアクセスを制御します。

VACM モードは NMS から MIB オブジェクトのアクセス権のみを必要とします。

snmp-agent community コマンドを使用して 10 個の SNMP コミュニティを作成することができます。コミュニティ名が同一で、ほかのパラメータが異なる設定を指定するため、コマンドを複数回実行する場合、最後に実行した設定が適用されます。

プレーンテキストでコミュニティを設定し、保存する場合、**simple** あるいは **cipher** を指定しないでください。

ACL は不正な NMS をフィルタするために使用します。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し､ACL にルールが存在する場合､ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細はオペレーションマニュアルのセクション 13 *セキュリティ“ACL”*を参照してください。

snmp-agent usm-user { v1 | v2c }コマンド、**snmp-agent group { v1 | v2c }**コマンドを使用して SNMP コミュニティを作成することができます。2 つのコマンドは SNMPv1 あるいは SNMPv2c ユーザ、ユーザが割り当てられるグループを作成します。システムは自動で SNMPv1 あるいは SNMPv2c ユーザ名を使用して SNMP コミュニティを作成します。

例

プレーンテキストで読み込み専用のコミュニティ readaccess を作成します。SNMPv1 あるいは SNMPv2c の NMS はデフォルト view の ViewDefault の MIB オブジェクトを読むため、コミュニティ readaccess を使用します。

<AP> system-view

[AP] snmp-agent sys-info version v1 v2c

[AP] snmp-agent community read simple readaccess

プレーンテキストで読み込み、書き込みコミュニティ writeaccess を作成します。SNMPv2c の IP アドレスが 1.1.1.1 の NMS はデフォルト view の ViewDefault の MIB オブジェクトを読み書きするため、コミュニティ writeaccess を使用します。

<AP> system-view

[AP] acl basic 2001

[AP-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0

[AP-acl-ipv4-basic-2001] rule deny source any

[AP-acl-ipv4-basic-2001] quit

[AP] snmp-agent sys-info version v2c

[AP] snmp-agent community write simple writeaccess acl 2001

プレーンテキストで読み込み、書き込みコミュニティ writeaccess を作成します。SNMPv2c の IP アドレスが 1.1.1.2 の NMS はデフォルト view の ViewDefault の MIB オブジェクトを読み書きするため、コミュニティ writeaccess を使用します。

<AP> system-view

[AP] acl basic name testacl

[AP-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0

[AP-acl-ipv4-basic-testacl] rule deny source any

[AP-acl-ipv4-basic-testacl] quit

[AP] snmp-agent sys-info version v2c

[AP] snmp-agent community write simple writeaccess acl name testacl

プレーンテキストで読み込み、書き込みコミュニティ wr-sys-acc を作成します。SNMPv1 あるいは SNMPv2c の NMS はシステムサブツリー（OID 1.3.6.1.2.1.1）の MIB オブジェクトを読み書きするため、コミュニティ wr-sys-acc を使用します。

<AP> system-view

[AP] snmp-agent sys-info version v1 v2c

[AP] undo snmp-agent mib-view ViewDefault

[AP] snmp-agent mib-view included test system

[AP] snmp-agent community write simple wr-sys-acc mib-view test

関連コマンド

- **display snmp-agent community**
- **snmp-agent mib-view**

3.1.15 snmp-agent group

Syntax

SNMPv1、SNMPv2c：

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *view-name*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent group { **v1** | **v2c** } *group-name*

SNMPv3：

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *view-name*] [**notify-view** *view-name*] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

group-name: SNMP グループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

authentication: SNMPv3 グループでプライバシーなしのモデルを指定します。

privacy: SNMPv3 グループでプライバシーセキュリティのモデルを指定します。

read-view *view-name*: 読み込み専用の MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。MIB view はアクセス可能な MIB オブジェクトの一式を示します。読み込み専用の MIB view を指定しない場合、SNMP グループはデフォルト MIB view の **ViewDefault** の MIB オブジェクトに問い合わせることができます。

write-view *view-name*: 読み込み、書き込みの MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。読み込み、書き込みの MIB view を指定しない場合、SNMP グループは SNMP エージェントの MIB オブジェクトを設定することができません。

notify-view *view-name*: notify の MIB view を指定します。*view-name* は MIB view の名前を示します。設定範囲は 1～32 文字です。SNMP エージェントは notify view に含まれる MIB オブジェクトのため、指定されたグループのみのユーザに通知を送信します。notify の MIB view を指定しない場合、SNMP グループは指定されたグループのユーザに通知を送信しません。

acl: 標準 IPv4 ACL コミュニティを指定します。

ipv4-acl-number: 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 IPv4 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

snmp-agent group コマンドは SNMP グループを作成し、アクセス権限を指定します。

undo snmp-agent group コマンドは SNMP グループを削除します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMP グループのすべてのユーザはセキュリティモデルとグループのアクセス権限を共有します。

SNMPv1 グループ、SNMPv2c グループ、SNMPv3 グループを含んで 20 個の SNMP グループを作成することができます。

グループのすべての SNMPv3 ユーザは同じセキュリティモデルを共有しますが、異なる認証とプライバシーセキュリティの設定を使用することができます。ユーザのセキュリティモデルを実装し、SNMP 通信の失敗を防ぐため、グループのセキュリティモデルの設定とユーザのセキュリティのキーの設定が、表 3-6 に従い、NMS の設定に一致していることを確認してください。

表 3-6 異なるセキュリティモデルの標準セキュリティの設定要件

セキュリティモデル	グループのセキュリティモデルのキーワード	ユーザのセキュリティのキーの設定	補足
プライバシーセキュリティあり、認証	**privacy**	認証キー、プライバシーキー	認証キーあるいはプライバシーセキュリティが設定されていない場合、SNMPの通信は失敗します。
プライバシーセキュリティなし、認証	**authentication**	暗号キー	認証キーが設定されていない場合、SNMPの通信は失敗します。 ユーザのプライバシーセキュリティ（ある場合）は影響しません。

セキュリティモデル	グループのセキュリティモデルのキーワード	ユーザのセキュリティのキーの設定	補足
プライバシーセキュリティなし、認証なし	**authentication**、**privacy** のどちらもありません、	なし	認証キーとプライバシーセキュリティが設定されても影響ありません。

ユーザ、グループのため、ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し、ACL にルールが存在する場合、ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細はオペレーションマニュアルのセクション 13 *セキュリティ“ACL”*を参照してください。

例

SNMPv3 グループ **group1** を作成します。

<AP> system-view

[AP] snmp-agent group v3 group1

関連コマンド

- **display snmp-agent group**
- **snmp-agent mib-view**
- **snmp-agent usm-user**

3.1.16 snmp-agent local-engineid

Syntax

snmp-agent local-engineid *engineid*

undo snmp-agent local-engineid

デフォルト

ローカルエンジン ID は company ID と device ID の組み合わせです。Device ID は製品によって異なります。

View

System view

定義済みユーザロール

network-admin

パラメータ

engineid: 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。

説明

snmp-agent local-engineid コマンドはローカル SNMP エージェントの SNMP エンジン ID を変更します。

undo snmp-agent local-engineid コマンドはデフォルトに戻します。

SNMP エンジン ID は SNMP が管理するネットワークで SNMP エンティティを固有に識別します。ローカル SNMP エンジン ID は通信の問題を防ぐため、SNMP が管理するネットワーク内で一意であることを確認してください。

SNMPv3 ユーザが設定されている場合、必要に応じてローカル SNMP エンジン ID を変更してください。変更すると設定した SNMPv3 ユーザ名と暗号化したキーを無効にすることができます。

例

ローカルエンジン ID を 123456789A に変更します。

<AP> system-view

[AP] snmp-agent local-engineid 123456789A

関連コマンド

- **display snmp-agent local-engineid**
- **snmp-agent usm-user**

3.1.17 snmp-agent log

Syntax

snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

undo snmp-agent log { **all** | **authfail** | **get-operation** | **set-operation** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

all: SNMP 認証失敗、Get オペレーション、Set オペレーションのロギングを有効にします。

authfail: SNMP 認証の失敗のロギングを有効にします。

get-operation: SNMP Get オペレーションのロギングを有効にします。

set-operation: SNMP Set オペレーションのロギングを有効にします。

説明

snmp-agent log コマンドは SNMP オペレーションのロギングを有効にします。

undo snmp-agent log コマンドは SNMP オペレーションのロギングを無効にします。

NMS のふるまいを検査するため、SNMP エージェントで実行された SNMP オペレーションを記録することができます。SNMP エージェントはログデータを information center に送信します。必要に応じて宛先にデータを出力するように Information Center を設定することができます。

例

SNMP Get オペレーションのロギングを有効にします。

<AP> system-view

[AP] snmp-agent log get-operation

SNMP Set オペレーションのロギングを有効にします。

<AP> system-view

[AP] snmp-agent log set-operation

SNMP 認証失敗のロギングを有効にします。

<AP> system-view

[AP] snmp-agent log authfail

3.1.18 snmp-agent mib-view

Syntax

snmp-agent mib-view { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

デフォルト

SNMP エージェントが有効なとき、システムは **ViewDefault** view を作成します。デフォルト MIB view では **iso** サブツリーのすべての MIB オブジェクトは **snmpUsmMIB**、**snmpVacmMIB**、**snmpModules.18** サブツリーを除いてアクセス可能です。

View

System view

定義済みユーザロール

network-admin

パラメータ

excluded: 指定した MIB サブツリーのすべてのノードへのアクセスを拒否します。

included: 指定した MIB サブツリーのすべてのノードへのアクセスを許可します。
view-name: view 名を指定します。設定範囲は 1～32 文字です。

oid-tree: ルートノードの OID（たとえば、**1.3.6.1.2.1.1**）あるいはオブジェクト名（たとえば、**system**）によって MIB サブツリーを指定します。設定範囲は 1～255 文字です。大文字、小文字を区別します。OID は MIB ツリーのオブジェクトを固有に識別するドットで区切られた数字です。

mask *mask-value*: MIB サブツリーのマスクを指定します。16 進数です。マスク長は 2～32 の偶数にする必要があります。

説明

snmp-agent mib-view コマンドは MIB view を作成あるいはアップデートします。

undo snmp-agent mib-view コマンドは MIB view を削除します。

MIB view は、アクセス制限のある MIB オブジェクトの集合（あるいは MIB オブジェクト階層）を示し、view 名によって識別されます。MIB view に含まれる MIB オブジェクトはアクセス可能ですが、MIB view から除外されている MIB オブジェクトはアクセスできません。

各 *view-name oid-tree* は view のレコードを示します。異なる MIB サブツリーのマスクで複数回、同一のレコードを指定する場合、最後に行った設定が適用されます。

デフォルト MIB view を削除する場合には注意してください。デフォルト view を使用する NMS から装置の MIB オブジェクトにアクセスできなくなります。

例

mibtest view に mib-2（OID 1.3.6.1.2.1）サブツリーを含め、この view から **system** サブツリーを除外します。

<AP> system-view

[AP] snmp-agent sys-info version v1

[AP] snmp-agent mib-view included mibtest 1.3.6.1.2.1

[AP] snmp-agent mib-view excluded mibtest system

[AP] snmp-agent community read public mib-view mibtest

コミュニティ **public** の SNMPv1 の NMS は **mib-2** サブツリーのオブジェクトに問い合わせすることができますが、**system** サブツリーの他のオブジェクト（たとえば、**sysDescr** あるいは **sysObjectID** ノード）は問い合わせすることができません。

関連コマンド

- **display snmp-agent mib-view**
- **snmp-agent group**

3.1.19 snmp-agent packet max-size

Syntax

snmp-agent packet max-size *byte-count*

undo snmp-agent packet max-size

デフォルト

1500 バイト

View

System view

定義済みユーザロール

network-admin

パラメータ

byte-count: SNMP エージェントが送受信できる SNMP パケットの最大サイズを指定します。設定範囲は 484～17940 バイトです。

説明

snmp-agent packet max-size コマンドは SNMP エージェントが送受信できる SNMP パケットの最大サイズを設定します。

undo snmp-agent packet max-size コマンドはデフォルトに戻します。

NMS へのパス上の装置がパケットのフラグメンテーションをサポートしていない場合、大きいサイズのパケットが廃棄されないようにするため、SNMP パケットサイズを制限します。通常のネットワークではデフォルトの設定で十分です。

例

SNMP パケットの最大サイズを 1024 バイトに設定します。

<AP> system-view

[AP] snmp-agent packet max-size 1024

3.1.20 snmp-agent sys-info contact

Syntax

snmp-agent sys-info contact *sys-contact*

undo snmp-agent sys-info contact

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

sys-contact: システム連絡先を指定します。設定範囲は 1～255 文字です。

説明

snmp-agent sys-info contact コマンドはシステム連絡先を設定します。

undo snmp-agent sys-info contact コマンドはデフォルトに戻します。

システム管理の連絡先と管理者を設定します。

例

システム連絡先を **Dial System Operator # 27345** に指定します。

<AP> system-view

[AP] snmp-agent sys-info contact Dial System Operator # 27345

関連コマンド

display snmp-agent sys-info

3.1.21 snmp-agent sys-info location

Syntax

snmp-agent sys-info location *sys-location*

undo snmp-agent sys-info location

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

sys-location: システム所在地を指定します。設定範囲は 1～255 文字です。

説明

snmp-agent sys-info location コマンドはシステム所在地を設定します。

undo snmp-agent sys-info location コマンドはデフォルトに戻します。

システム管理の装置と管理者の所在地を設定します。

例

システム所在地を **Room524-row1-3** に設定します。

<AP> system-view

[AP] snmp-agent sys-info location Room524-row1-3

関連コマンド

display snmp-agent sys-info

3.1.22 snmp-agent sys-info version

Syntax

snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

undo snmp-agent sys-info version { **all** | { **v1** | **v2c** | **v3** } * }

デフォルト

SNMPv3

View

System view

定義済みユーザロール

network-admin

パラメータ

all: SNMPv1、SNMPv2c、SNMPv3 を指定します。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

説明

snmp-agent sys-info version コマンドは SNMP のバージョンを有効にします。

undo snmp-agent sys-info version コマンドは SNMP のバージョンを無効にします。

NMS が SNMP エージェントと正常に通信するため、SNMP エージェントは NMS と同じ SNMP のバージョンを設定します。

例

SNMPv3 を有効にします。

<AP> system-view

[AP] snmp-agent sys-info version v3

関連コマンド

display snmp-agent sys-info

3.1.23 snmp-agent target-host

Syntax

snmp-agent target-host inform address udp-domain *ipv4-address* [**udp-port** *port-number*] **params securityname** *security-string* { **v2c** | **v3** [**authentication** | **privacy**] }

snmp-agent target-host trap address udp-domain *ipv4-address* [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { **trap** | **inform** } **address udp-domain** *ipv4-address* **params securityname** *security-string*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

inform: inform として通知を送信します。

trap: trap として通知を送信します。

address: SNMP 通知の宛先アドレスを指定します。

udp-domain: トランスポートプロトコルとして UDP を指定します。

ipv4-address: SNMP 通知の宛先として、ターゲットホストの IPv4 アドレスあるいはホスト名を指定します。ホスト名の設定範囲は 1～253 文字です。大文字、小文字を区別しません。英字、数字、ハイフン（-）、アンダーライン（_）、ドット（.）を含むことができます。ホスト名を指定する場合、ターゲットホストの IPv4 アドレスは、取得することができます。

udp-port *port-number*: SNMP 通知の UDP ポートを指定します。指定しない場合、UDP ポート 162 が使用されます。

params securityname *security-string*: 認証パラメータを指定します。*security-string* は SNMPv1 コミュニティ、SNMPv2c コミュニティ、あるいは SNMPv3 ユーザ名を指定します。設定範囲は 1～32 文字です。

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

v3: SNMPv3 を指定します。

- **authentication**: プライバシーセキュリティなしで認証するようにセキュリティモデルを指定します。SNMPv3 ユーザを作成したとき認証キーを指定する必要があります。
- **privacy**: プライバシーセキュリティありで認証するようにセキュリティモデルを指定します。SNMPv3 ユーザを作成したとき認証キーとプライバシーキーを指定する必要があります。

説明

snmp-agent target-host コマンドは SNMP 通知（inform あるいは trap）をホストに送信するため、SNMP エージェントを設定します。

undo snmp-agent target-host コマンドは SNMP 通知のターゲットホストを削除します。

複数の SNMP 通知のターゲットホストを指定することができます。

SNMP エージェントは SNMP 通知のため、ターゲットホストの UDP ポートと同一のポートを使用する必要があります。通常、MIB ブラウザのような NMS は SNMP 通知のために、SNMP プロトコルで定義された UDP ポート 162 を使用します。

v1、**v2c**、**v3** を指定しない場合、SNMPv1 が使用されます。ホストが通知を受信できるように、SNMP エージェントは、ターゲットホストの SNMP のバージョンと同一のバージョンを使用することを確認してください。

authentication あるいは **privacy** の両方を指定しない場合、セキュリティモデルはプライバシーセキュリティなし、認証なしです。

例

ユーザ **public** の 10.1.1.1 に SNMPv3 の trap を送信するため、SNMP エージェントを設定します。

<AP> system-view

[AP] snmp-agent trap enable standard

[AP] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname public v3

関連コマンド

- **snmp-agent { inform | trap } source**
- **snmp-agent trap enable**
- **snmp-agent trap life**

3.1.24 snmp-agent trap enable

Syntax

snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

undo snmp-agent trap enable [**configuration** | *protocol* | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] * | **system**]

デフォルト

SNMP configuration 通知、standard 通知、system 通知は有効です。他の SNMP 通知はモジュールによって変わります。

View

System view

定義済みユーザロール

network-admin

パラメータ

configuration: configuration 通知を指定します。configuration 通知が有効である場合、システムはカレントコンフィグレーションとスタートアップコンフィグレーションを 10 分毎に変更点を確認し、最新の変更の通知を作成します。

protocol: SNMP 通知が有効なモジュールを指定します。このパラメータの詳細は各モジュールのコマンドマニュアルを参照してください。

standard: standard 通知を指定します。

表 3-7 Standard SNMP 通知

キーワード	定義
authentication	NMSがSNMPエージェントへの認証に失敗したとき、認証失敗通知を送信します。
coldstart	装置が再起動したときに通知を送信します。
linkdown	ポートのリンクがダウンしたときに通知を送信します。
linkup	ポートのリンクがアップしたときに通知を送信します。
warmstart	SNMPエージェントが再起動したときに通知を送信します。

system: システム時間が変更された、システムが再起動した、あるいはメインのシステムソフトウェアイメージが有効でないときに system 通知を指定します。

説明

snmp-agent trap enable コマンドは SNMP 通知を有効にします。

undo snmp-agent trap enable コマンドは SNMP 通知を無効にします。

重大なプロトコルのイベントを NMS に通知するため、プロトコルの SNMP 通知を有効にしてください。SNMP 通知を正常に送信するため、必要な Notification のパラメータを設定してください。notification は trap、inform が含まれます。trap パラメータを使用した場合でも notification には trap、inform が含まれます。

装置がホストに inform、trap の notification を送信する場合、**snmp-agent target-host** コマンドを使用することができます。

例

SNMP 認証の失敗の Notification を送信するように SNMP エージェントを有効にします。

<AP> system-view

[AP] snmp-agent trap enable standard authentication

関連コマンド

snmp-agent target-host

3.1.25 snmp-agent trap if-mib link extended

Syntax

snmp-agent trap if-mib link extended

undo snmp-agent trap if-mib link extended

デフォルト

SNMP エージェントは標準 linkUp/linkDown 通知を送信します。

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap if-mib link extended コマンドは拡張 linkUp/linkDown 通知を送信するように SNMP エージェントを設定します。

undo snmp-agent trap if-mib link extended コマンドはデフォルトに戻します。

拡張 linkUp/linkDown 通知は、早急に故障個所を識別するため、標準 linkUp/linkDown 通知にインタフェースの説明とインタフェースのタイプを追加します。

このコマンドを使用するとき、NMS が拡張 linkUp/linkDown 通知をサポートしていることを確認してください。

例

拡張 linkUp/linkDown 通知を送信するように SNMP エージェントを設定します。

<AP> system-view

[AP] snmp-agent trap if-mib link extended

3.1.26 snmp-agent trap life

Syntax

snmp-agent trap life *seconds*

undo snmp-agent trap life

デフォルト

120 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

seconds: ライフタイムを指定します。設定範囲は 1～2592000 秒です。

説明

snmp-agent trap life コマンドはSNMP通知キューの通知のライフタイムを設定します。

undo snmp-agent trap life コマンドはデフォルトの通知のライフタイムに戻します。

衝突が発生すると、SNMP エージェントはキューに通知をバッファします。通知のライフタイムはキューに保持しておく期間を設定します。ライフタイムが終了したとき notification は削除されます。

例

SNMP 通知のライフタイムを 60 秒に設定します。

<AP> system-view

[AP] snmp-agent trap life 60

関連コマンド

- **snmp-agent target-host**
- **snmp-agent trap enable**
- **snmp-agent trap queue-size**

3.1.27 snmp-agent trap log

Syntax

snmp-agent trap log

undo snmp-agent trap log

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

snmp-agent trap log コマンドは SNMP 通知のロギングを有効にします。

undo snmp-agent trap log コマンドは SNMP 通知のロギングを無効にします。

通知のトラッキングを行うため、SNMP エージェントによって送信された SNMP 通知を記録するため、SNMP 通知のロギングを使用します。SNMP エージェントは Information Center にログを送信します。必要に応じて宛先にログを出力するように Information Center を設定することができます。

例

SNMP 通知のロギングを有効にします。

<AC> system-view

[AC] snmp-agent trap log

3.1.28 snmp-agent trap queue-size

Syntax

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

デフォルト

100

View

System view

定義済みユーザロール

network-admin

パラメータ

size: SNMP 通知のキューが保持できる通知の最大数を指定します。設定範囲は 1～1000 です。

説明

snmp-agent trap queue-size コマンドは SNMP 通知のキューのサイズを設定します。

undo snmp-agent trap queue-size コマンドはデフォルトのキューのサイズに戻します。

衝突が発生したとき、SNMP エージェントはキューに通知をバッファします。SNMP 通知のキューのサイズは SNMP 通知のキューが保持できる通知の最大数を設定します。キューのサイズが上限に到達したとき、新しい通知のために、古い通知が廃棄されます。

例

SNMP 通知のキューのサイズを 200 に設定します。

<AP> system-view

[AP] snmp-agent trap queue-size 200

関連コマンド

- **snmp-agent target-host**
- **snmp-agent trap enable**
- **snmp-agent trap life**

3.1.29 snmp-agent usm-user { v1 | v2c }

Syntax

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent usm-user { **v1** | **v2c** } *user-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

v1: SNMPv1 を指定します。

v2c: SNMPv2c を指定します。

user-name: SNMP ユーザ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

group-name: SNMPv1 あるいは SNMPv2c のグループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。グループは、すでに作成されたものでも指定できます。グループが作成されていない場合、グループを作成した後、適用されます。

acl: 標準 IPv4 ACL を指定します。

ipv4-acl-number: 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 IPv4 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

説明

snmp-agent usm-user { **v1** | **v2c** }コマンドは SNMPv1 あるいは SNMPv2c グループにユーザを追加します。

undo snmp-agent usm-user { **v1** | **v2c** }コマンドは SNMPv1 あるいは SNMPv2c グループからユーザを削除します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMPv1 あるいは SNMPv2c では NMS エージェントはコミュニティ名を使用して互いに認証します。SNMPv3 ではユーザ名を使用して互いに認証します。

以下のどちらかの方法を使用して SNMPv1 あるいは SNMPv2c コミュニティを作成することができます。

- **snmp-agent community** コマンドを実行します。
- SNMPv1 あるいは SNMPv2c ユーザ、ユーザに割り当てられるグループを作成するため、**snmp-agent usm-user { v1 | v2c }**コマンド、**snmp-agent group { v1 | v2c }** コマンドを実行します。システムは SNMPv1 あるいは SNMPv2c のユーザ名を使用して自動で SNMP コミュニティを作成します。

ユーザ、グループのために ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し、ACL にルールが存在する場合、ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細はオペレーションマニュアルのセクション 13 *セキュリティ "ACL"* を参照してください。

例

NMS が SNMPv2c を使用するため、SNMPv2c グループ **readCom** にユーザ **userv2c** を追加します。読み込み専用のコミュニティ **userv2c** を使用して装置にアクセスします。

<AP> system-view

[AP] snmp-agent sys-info version v2c

[AP] snmp-agent group v2c readCom

[AP] snmp-agent usm-user v2c userv2c readCom

IP アドレス 1.1.1.1 の NMS が SNMPv2c を使用するため、SNMPv2c グループ **readCom** にユーザ **userv2c** を追加します。読み込み専用のコミュニティ **userv2c** を使用して装置にアクセスします。

<AP> system-view

[AP] acl basic 2001

[AP-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0.0.0.0

[AP-acl-ipv4-basic-2001] rule deny source any

[AP-acl-ipv4-basic-2001] quit

[AP] snmp-agent sys-info version v2c

[AP] snmp-agent group v2c readCom

[AP] snmp-agent usm-user v2c userv2c readCom acl 2001

IP アドレス 1.1.1.2 の NMS が SNMPv2c を使用するため、SNMPv2c グループ **readCom** にユーザ **userv2c** を追加します。読み込み専用のコミュニティ **userv2c** を使用して装置にアクセスします。

[AP] acl basic name testacl

[AP-acl-ipv4-basic-testacl] rule permit source 1.1.1.2 0.0.0.0

[AP-acl-ipv4-basic-testacl] rule deny source any

[AP-acl-ipv4-basic-testacl] quit

[AP] snmp-agent sys-info version v2c

[AP] snmp-agent group v2c readCom

[AP] snmp-agent usm-user v2c userv2c readCom acl name testacl

関連コマンド

- **display snmp-agent community**
- **snmp-agent community**
- **snmp-agent group**

3.1.30 snmp-agent usm-user v3

Syntax

snmp-agent usm-user v3 *user-name group-name* [{ **cipher** | **simple** } **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** { *ipv4-acl-number* | **name** *ipv4-acl-name* }] *

undo snmp-agent usm-user v3 *user-name* { **local** | **engineid** *engineid-string* }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

user-name: SNMPv3 ユーザ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

group-name: SNMPv3 のグループ名を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。グループが作成されていない場合、ユーザはグループが作成されたのち適用されます。

cipher: 認証キーと暗号化キーを暗号テキストとして指定します。キーは暗号テキストで保存されます。

simple: 認証キーと暗号化キーをプレーンテキストとして指定します。

authentication-mode: 認証アルゴリズムを指定します。指定しない場合、認証を行いません。

- **md5**: HMAC-MD5 認証アルゴリズムを指定します。
- **sha**: HMAC-SHA1 認証アルゴリズムを指定します。

auth-password: 認証キーを指定します。大文字、小文字を区別します。

- プレーンテキストの設定範囲は 1～64 文字です。数字、大文字、小文字、記号を含む必要があります。
- キーの暗号テキストは **snmp-agent calculate-password** コマンドで計算されます。

privacy-mode: 暗号アルゴリズムを指定します。指定しない場合、暗号を行いません。

- **3des**: 168 ビットのキーを使用して 3DES アルゴリズムを指定します。
- **aes128**: 128 ビットのキーを使用して AES アルゴリズムを指定します。
- **des56:** 56 ビットのキーを使用して DES アルゴリズムを指定します。

priv-password: 暗号キーを指定します。大文字、小文字を区別します。

- プレーンテキストの設定範囲は 1～64 文字です。数字、大文字、小文字、記号を含む必要があります。
- キーの暗号テキストは **snmp-agent calculate-password** コマンドで計算されます。

acl: 標準 IPv4 ACL を指定します。

ipv4-acl-number: 標準 IPv4 ACL 番号を指定します。設定範囲は 2000～2999 です。

name *ipv4-acl-name*: 標準 IPv4 ACL 名を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別しません。

local: ローカル SNMP エンジンを指定します。デフォルトで SNMPv3 ユーザはローカル SNMP エンジンに関連づけられています。

engineid *engineid-string*: 16 進数の文字列で SNMP エンジン ID を指定します。文字列の長さは偶数で構成する必要があります。設定範囲は 10～64 です。すべて 0 あるいはすべて F の文字列は無効です。ローカルエンジンの ID を変更した後、既存の SNMPv3 ユーザと暗号化されたキーは無効になります。無効なユーザ名を削除する場合、**undo snmp-agent usm-user v3** コマンドでユーザ名にエンジン ID を指定してください。

再度設定を行う必要があります。

説明

snmp-agent usm-user v3 コマンドは SNMPv3 にユーザを作成します。

undo snmp-agent usm-user v3 コマンドは SNMPv3 からユーザを削除します。

コマンドはユーザロールが network-admin あるいは level-15 のみ実行することができます。これらのロールがほかのユーザロールでは SNMP 機能やコマンドの使用を許可されたとしても実行することができません。

SNMPv3 ユーザで MIB オブジェクトにアクセスを制御するため、以下のモードを使用することができます。

- **VACM（View ベースアクセス制御モデル）**—VACM モードはグループに SNMPv3 ユーザを割り当てる前に SNMPv3 グループを作成する必要があります。そうでない場合、グループが作成されたのち、ユーザが適用されません。SNMP グループは複数のユーザを含むことができます。SNMP グループはユーザのグループの MIB view とセキュリティモデルを指定します。各ユーザの認証と暗号化アルゴリズムは作成されたときに指定されます。

異なる SNMPv3 ユーザを作成するため **snmp-agent usm-user v3** コマンドを複数設定することができます。ユーザ名が同一である場合、最後に行った設定が適用されます。

NMS でエージェントにアクセスする場合、以下のことが必要です。

ユーザ、グループのために ACL は不正な NMS をフィルタするために使用します。ユーザ、グループの両方で ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

- ACL を指定しない、指定した ACL が存在しない、ACL にルールがない場合、すべての NMS は SNMP エージェントにアクセスすることができます。
- ACL を指定し、ACL にルールが存在する場合、ACL に許可された NMS のみが SNMP エージェントにアクセスすることができます。

ACL の詳細はオペレーションマニュアルのセクション 13 *セキュリティ“ACL”*を参照してください。

例

SNMPv3 グループ **testGroup** にユーザ **testUser** を追加します。グループでプライバシーセキュリティモデルなしで認証を有効にします。ユーザの認証アルゴリズムを HMAC-SHA11、プレーンテキストで認証キーを **123456TESTplat&!**に設定します。

<AP> system-view

[AP] snmp-agent group v3 testGroup authentication

[AP] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTplat&!

デフォルト view が **ViewDefault** の MIB オブジェクトに NMS がアクセスするため、SNMP エージェントの設定と同様に以下の NMS の設定を行います。

- SNMPv3 ユーザ名
- SNMP プロトコルバージョン
- 認証アルゴリズムとキー

SNMPv3 グループ **testGroup** にユーザ **testUser** を追加します。グループで認証とプライバシーセキュリティモデルを有効にします。ユーザの認証アルゴリズムを HMAC-SHA1、プライバシーアルゴリズムを AES、プレーンテキストで認証キーを **123456TESTauth&!**に設定します。プレーンテキストでユーザのプライバシーキーを **123456TESTencr&!**に設定します。

<AP> system-view

[AP] snmp-agent group v3 testGroup privacy

[AP] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!

デフォルト view が **ViewDefault** の MIB オブジェクトに NMS がアクセスするため、SNMP エージェントの設定と同様に以下の NMS の設定を行います。

- SNMPv3 ユーザ名
- SNMP プロトコルバージョン
- 認証アルゴリズム

関連コマンド

- **display snmp-agent usm-user**
- **snmp-agent calculate-password**
- **snmp-agent group**

目次

このセクションのページは **15-x-x** です。

4 章 NETCONF 4-1
4.1 NETCONF 設定コマンド 4-1
4.1.1 netconf log 4-1
4.1.2 netconf soap http enable 4-4
4.1.3 netconf soap https enable 4-5
4.1.4 netconf ssh server enable 4-6
4.1.5 xml 4-7

4章 NETCONF

4.1 NETCONF設定コマンド

4.1.1 netconf log

Syntax

netconf log source { **all** | { **agent** | **soap** | **web** } * } { **protocol-operation** { **all** | { **action** | **config** | **get** | **session** | **set** | **syntax** | **others** } * } | **row-operation** | **verbose** }

undo netconf log source { { **soap** | **web** } * } { { **protocol-operation** { **all** | { **action** | **config** | **get** | **set** | **session** | **syntax** | **others** } * } } | **verbose** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

source: NETCONF オペレーションを実行するクライアントプロトコルを指定します。

- **all**: すべてのプロトコルを使用する NETCONF クライアントを指定します。
- **soap**: SOAP over HTTP 、あるいは SOAP over HTTPS を使用しているクライアントを指定します。
- **web**: Web を使用しているクライアントを指定します。
- **protocol-operation:** NETCONF オペレーションタイプを指定します。
- **all**: 全ての NETCONF オペレーションを指定します。
- **action**: action オペレーションを指定します。
- **config**: NETCONF のコンフィグオペレーションを指定します。CLI、save、load、rollback、lock、unlock と save-point オペレーションを含みます。
- **get**: 情報取得に関する NETCONF オペレーションを指定します。get、get-config、get-bulk、get-bulk-config と get-sessions オペレーションを含みます。
- **set**: 全ての edit-config オペレーションを指定します。
- **session**: セッションに関する NETCONF オペレーションを指定します。kill-session、close-session と hello メッセージの capability 交換を含みます。
- **syntax**: XML と schema のエラーを指定します。
- **others**: action、config、get、set、session と syntax 以外の NETCONF オペレーションを指定します。

row-operation: action および edit-config オペレーションの行操作をログに記録します。

verbose: NETCONF 情報の詳細なログを出力します。リクエストに関するオペレーションでは、簡易な情報に続いてリクエストのテキストのログを出力します。サービスに関するオペレーションでは、edit-config についてのみ有効です。edit-config でエラーが発生した場合、エラーの詳細情報を出力します。

説明

netconf log コマンドは NETCONF ロギングを有効にします。

undo netconf log コマンドは NETCONF ロギングを無効にします。

protocol-operation キーワードを指定すると、一致した動作と動作結果がそれぞれデバイスに記録されます。たとえば、NETCONF 操作を実行して VLAN 3~5 を作成すると、デバイスは次のログメッセージを出力します。

```
%Mar 21 17:11:34:479 2017 Sysname XMLSOAP/6/XML_REQUEST: test from
192.168.100.198,
session id 2,message-id 100, receive edit-config request.
%Mar 21 17:11:34:483 2017 Sysname XMLSOAP/6/EDIT-CONFIG: test from
192.168.100.198,
session id 2,message-id 100, execute success.
```

row-operation キーワードを指定すると、装置は action または edit-config オペレーションの各行操作と操作結果をログに記録します。たとえば、NETCONF オペレーションを実行して VLAN 3~5 を作成すると、装置は次のログメッセージを出力します。

```
%Mar 31 17:50:02:608 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test,
192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=3),
result=Succeeded. No
attributes.
%Mar 31 17:50:02:609 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test,
192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=4),
result=Succeeded. No
attributes.
%Mar 31 17:50:02:611 2017 Sysname XMLSOAP/6/EDIT-CONFIG: User (test,
192.168.100.20,
session ID 1), message ID=100, operation=create VLAN/VLANs (ID=5),
result=Succeeded. No
attributes.
```

NETCONF で作成されたログを Information Center に正しく送信するため、Information Center の設定を行う必要があります。詳細はオペレーションマニュアルのセクション 2 *システム管理 “Information Center”* を参照してください。

例

クライアントからの edit-config 情報について、NETCONF のログを出力するように設定します。

<AP> system-view

[AP] netconf log source web protocol-operation set

例

IPv4 ACL 2001 を使用して、サブネット 10.10.0.0/16 の NETCONF クライアントのみが NETCONF over SOAP over HTTP session を確立できるようにします。

```
<AP> system-view
[AP] acl basic 2001
[AP-acl-ipv4-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[AP-acl-ipv4-basic-2001] quit
[AP] netconf soap http acl 2001
```

4.1.2 netconf soap http enable

Syntax

netconf soap http enable

undo netconf soap http enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

netconf soap http enable コマンドは NETCONF over SOAP を有効にします。

このコマンドを実行すると、装置は HTTP パケット中の SOAP（Simple Object Access Protocol）でカプセル化された NETCONF メッセージを解釈するようになります。

例

NETCONF over SOAP over HTTP を有効にします。

<AP> system-view

[AP] netconf soap http enable

4.1.3 netconf soap https enable

Syntax

netconf soap https enable

undo netconf soap https enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

netconf soap https enable コマンドは NETCONF over SOAP を有効にします。

このコマンドを実行すると、装置は HTTPS パケット中の SOAP（Simple Object Access Protocol）でカプセル化された NETCONF メッセージを解釈するようになります。

例

NETCONF over SOAP over HTTPS を有効にします。

<AP> system-view

[AP] netconf soap https enable

4.1.4 netconf ssh server enable

Syntax

netconf ssh server enable

undo netconf ssh server enable

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

説明

netconf ssh server enable コマンドは SSH 経由での NETCONF 通信を有効にします。

undo netconf ssh server enable コマンドは SSH 経由での NETCONF 通信を無効にします。この機能を使用すると、SSH クライアントを使用して、NETCONF を SSH サブシステムとして呼び出すことができます。つまり、XML メッセージを直接使用して、xml コマンドを使用せずに NETCONF 操作を実行できます。

このコマンドを実行する前に、ユーザの認証モードをデバイスのスキームとして設定します。その後、SSH 経由の NETCONF 対応ユーザ端末は、SSH 経由で NETCONF を介してデバイスにアクセスすることができます。

機能セット **urn:ietf:params:netconf:base:1.0** のみが使用可能です。これは、デバイスとユーザ端末の両方でサポートされています。

例

SSH で NETCONF を有効にします。

<AP> system-view

[AP] Netconf ssh server enable

4.1.5 xml

Syntax

xml

View

User view

定義済みユーザロール

network-admin

network-operator

説明

xml コマンドは XML view に移行します。

XML view では、デバイスの設定や、デバイスからの情報取得を行う NETCONF メッセージを使用することができます。操作可能な NETCONF オペレーションはユーザロールに依存し、下表のとおりです。

表 4-1 操作可能な NETCONF オペレーションとユーザロール

フィールド	説明
network-admin	NETCONFオペレーション全てです。
network-operator	記憶媒体のタイプです。 ● Get ● Get-bulk ● Get-bulk-config ● Get-config ● Get-sessions ● Close-session

XML view の NETCONF メッセージのフォーマットを保証するため、NETCONF メッセージを手動で入力するのではなく、コピー&ペーストを行ってください。

NETCONF オペレーションを実行する際、NETCONF メッセージのペーストや Enter キーを押下するなどのほかのオペレーションを行わないでください。

NETCONF メッセージを識別するため、各 NETCONF メッセージの最後にエンドマーク“]]>]]>”を追加してください。

XML view に移行した後、装置は自動でクライアントに NETCONF の機能をアドバタイズします。NETCONF 機能をサポートしている装置に通知するため、クライアントを設定

してください。機能の交換を行った後、クライアントを使用して装置を設定することができます。

NETCONF メッセージは XML フォーマットに従い、装置の NETCONF XML API リファレンスの意味、構文に合致している必要があります。設定が正しく行われるようにするためには、NETCONF メッセージを生成する他社製ソフトウェアを使用することを推奨します。

XML view を終了するには、**quit** コマンドではなく、NETCONF メッセージを使用してください。

user line/user line class view において **escape-key** コマンド（デフォルトで CTRL+C）でショートカットキーを設定している場合、NETCONF メッセージにはショートカットキーを含むことができません。

NETCONF メッセージにショートカットキーが含まれる場合、XML view で関連する設定が影響を受ける可能性があります。たとえば、user line view で **escape-key a** コマンドを使用してショートカットキー“a”を設定した場合、NETCONF メッセージには文字“a”が含まれます。メッセージの最後の“a”のあとの内容のみを処理することができます。

例

XML view に移行します。

<AP> xml

```
<?xml version="1.0" encoding="UTF-8"?><hello
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"><capabilities><capability>urn
:ietf:params:netconf:base:1.1</capability><capability>urn:ietf:params:netconf
:writable-running</capability><capability>urn:ietf:params:netconf:capability:
notification:1.0</capability><capability>urn:ietf:params:netconf:capability:v
alidate:1.1</capability><capability>urn:ietf:params:netconf:capability:interl
eave:1.0</capability><capability>urn:ietf:params:netconf:capability:nec-netco
nf-ext:1.0</capability></capabilities><session-id>1</session-id></hello>]]>]]
>
```

XML view を終了します。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session>
  </close-session>
</rpc>]]>]]>
```

<AP>

目次

このセクションのページは **15-x-x** です。

5 章 プロセスモニタリングとメンテナンス 5-1
5.1 プロセスモニタリングとメンテナンス設定コマンド 5-1
5.1.1 display exception context 5-1
5.1.2 display exception filepath 5-7
5.1.3 exception filepath 5-8
5.1.4 process core 5-9
5.1.5 reset exception context 5-11

5章 プロセスモニタリングとメンテナンス

5.1 プロセスモニタリングとメンテナンス設定コマンド

5.1.1 display exception context

Syntax

display exception context [**count** *value*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

count *value*: コンテキスト情報のエントリを指定します。設定範囲は 1～20 です。デフォルトは 1 です。

説明

display exception context コマンドはプロセス例外に関するコンテキスト情報を表示します。

システムは、各コアファイルのコンテキスト情報エントリを作成します。コンテキスト情報エントリは、プロセス ID、クラッシュ時間、コアファイルのディレクトリ、スタック情報、レジスタ情報が含まれます。

例

x86 ベースの 32 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AP> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 120 (routed)
Crash signal: SIGBUS
Crash time: Tue Apr  9 17:14:30 2013
Core file path:
flash:/core/node0_routed_120_7_20130409-171430_1365527670.core
#0  0xb7caba4a
#1  0x0804cb79
#2  0xb7cd77c4
#3  0x08049f45
```

```
Backtrace stopped.
                    Registers' content
  eax:0xfffffffc   ebx:0x00000003   ecx:0xbfe244ec   edx:0x0000000a
  esp:0xbfe244b8   ebp:0xbfe244c8   esi:0xffffffff   edi:0xbfe24674
  eip:0xb7caba4a eflag:0x00000292    cs:0x00000073    ss:0x0000007b
   ds:0x0000007b    es:0x0000007b    fs:0x00000000    gs:0x00000033
```

x86 ベースの 64 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AP> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 121 (routed)
Crash signal: SIGBUS
Crash time: Sun Mar 31 11:12:21 2013
Core file path:
flash:/core/node0_routed_121_7_20130331-111221_1364728341.core
#0  0x00007fae7dbad20c
#1  0x00000000004059fa
#2  0x00007fae7dbd96c0
#3  0x0000000000402b29
Backtrace stopped.
                    Registers' content
      rax:0xfffffffffffffffc      rbx:0x00007fff88a5dd10
      rcx:0xffffffffffffffff      rdx:0x000000000000000a
      rsi:0x00007fff88a5dd10      rdi:0x0000000000000003
      rbp:0x00007fff88a5dcf0      rsp:0x00007fff88a5dcf0
       r8:0x00007fae7ea587e0       r9:0x0000000000000079
      r10:0xffffffffffffffff      r11:0x0000000000000246
      r12:0x0000000000405b18      r13:0x00007fff88a5ff7a
      r14:0x00007fff88a5de30      r15:0x0000000000000000
      rip:0x00007fae7dbad20c     flag:0x0000000000000246
       cs:0x0000000000000033       ss:0x000000000000002b
       ds:0x0000000000000000       es:0x0000000000000000
       fs:0x0000000000000000       gs:0x0000000000000000
   fs_base:0x00007fae80a5d6a0   gs_base:0x0000000000000000
   orig_ax:0x00000000000000e8
```

Power PC ベースの 32 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AP> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 133 (routed)
Crash signal: SIGBUS
```

```
Crash time: Wed Apr 10 15:47:49 2013
Core file path:
flash:/core/node0_routed_133_7_20130410-154749_1365608869.core
#0  0x184720bc
#1  0x10006b4c
Backtrace stopped.
                    Registers' content
grp00: 0x000000ee 0x7ffd6ad0 0x1800f440 0x00000004
grp04: 0x7ffd6af8 0x0000000a 0xffffffff 0x184720bc
grp08: 0x0002d200 0x00000003 0x00000001 0x1847209c
grp12: 0x10006b4c 0x10020534 0xd6744100 0x00000000
grp16: 0x00000000 0xa0203ff0 0xa028b12c 0xa028b13c
grp20: 0xa028b148 0xa028b168 0xa028b178 0xa028b190
grp24: 0xa028b1a8 0xa028b1b8 0x00000000 0x7ffd6c08
grp28: 0x10006cac 0x7ffd6f92 0x184c1b84 0x7ffd6ae0

 nip:0x184720bc   lr:0x10006b4c   cr:0x38000022   ctr:0x1847209c
 msr:0x0002db00  xer:0x00000000  ret:0xfffffffc dsisr:0x08000000
 gr3:0x00000003   mq:0x00000000 trap:0x00000c00  dar:0x1833114c
```

Power PC ベースの 64 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AP> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 172 (routed)
Crash signal: SIGBUS
Crash time: Sat Sep 15 16:53:16 2007
Core file path:
flash:/core/node1_routed_172_7_20070915-165316_1189875196.core
#0  0x00000fff803c66b4
#1  0x0000000010009b94
#2  0x00000fff80401814
Backtrace stopped.
                    Registers' content
    grp00: 0x00000000000000ee 0x00000fffffd04840
    grp02: 0x00000fff80425c28 0x0000000000000004
    grp04: 0x00000fffffd048c0 0x000000000000000a
    grp06: 0xffffffffffffffff 0x00000fff803c66b4
    grp08: 0x000000008002d000 0x0000000000000000
    grp10: 0x0000000000000000 0x0000000000000000
    grp12: 0x0000000000000000 0x00000fff80a096b0
    grp14: 0x000000007b964c00 0x000000007b7d0000
```

```
    grp16: 0x0000000000000001 0x000000000000000b
    grp18: 0x0000000000000031 0x0000000000a205b8
    grp20: 0x0000000000a20677 0x0000000000000000
    grp22: 0x000000007bb91014 0x0000000000000000
    grp24: 0xc0000000005ae1c8 0x0000000000000000
    grp26: 0xc0000001f00bff20 0xc0000001f00b0000
    grp28: 0x00000fffffd04a30 0x000000001001aed8
    grp30: 0x00000fffffd04fae 0x00000fffffd04840

     nip:0x00000fff803c66b4      lr:0x0000000010009b94
      cr:0x0000000058000482     ctr:0x00000fff803c66ac
     msr:0x000000008002d000     xer:0x0000000000000000
     ret:0xfffffffffffffffc   dsisr:0x0000000000000000
     gr3:0x0000000000000003   softe:0x0000000000000001
    trap:0x0000000000000c00     dar:0x00000fff8059d14c
```

MIPS ベースの 32 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AP> display exception context

```
Index 1 of 1
------------------------------
Crashed PID: 182 (routed)
Crash signal: SIGBUS
Crash time: Sun Jan  2 08:11:38 2013
Core file path:
flash:/core/node4_routed_182_10_20130102-081138_1293955898.core
#0  0x2af2faf4
#1  0x00406d8c
Backtrace stopped.
                    Registers' content
 zero:0x00000000   at:0x1000dc00   v0:0x00000004   v1:0x00000003
   a0:0x00000003   a1:0x7fd267e8   a2:0x0000000a   a3:0x00000001
   t0:0x00000000   t1:0xcf08fa14   t2:0x80230510   t3:0xffffff8
   t4:0x69766520   t5:0x00000000   t6:0x63cc6000   t7:0x44617461
   s0:0x7fd26f81   s1:0x00401948   s2:0x7fd268f8   s3:0x803e1db0
   s4:0x803e1da0   s5:0x803e1d88   s6:0x803e1d70   s7:0x803e1d60
   t8:0x00000008   t9:0x2af2fae0   k0:0x00000000   k1:0x00000000
   gp:0x2af9a3a0   sp:0x7fd267c0   s8:0x7fd267c0   ra:0x00406d8c
   sr:0x0000dc13   lo:0xef9db265   hi:0x0000003f  bad:0x2add2010
cause:0x00800020   pc:0x2af2faf4
```

MIPS ベースの 64 ビット端末のプロセス例外に関するコンテキスト情報を表示します。

<AP> display exception context

```
Index 1 of 1
------------------------------
```

```
Crashed PID: 270 (routed)
Crash signal: SIGBUS
Crash time: Wed Mar 27 12:39:12 2013
Core file path:
flash:/core/node16_routed_270_10_20130327-123912_1364387952.core
#0  0x0000005555a3bcb4
#1  0x0000000120006c1c
Backtrace stopped.
                    Registers' content
     zero:0x0000000000000000      at:0x0000000000000014
       v0:0x0000000000000004      v1:0x0000000000000003
       a0:0x0000000000000003      a1:0x000000ffff899d90
       a2:0x000000000000000a      a3:0x0000000000000001
       a4:0x0000005555a9b4e0      a5:0x0000000000000000
       a6:0xffffffff8021349c      a7:0x20696e206368616e
       t0:0x0000000000000000      t1:0xffffffff80105068
       t2:0xffffffff80213890      t3:0x0000000000000008
       s0:0x0000005555a99c40      s1:0x000000ffff89af5f
       s2:0x0000000120007320      s3:0x0000005555a5f470
       s4:0x000000ffff899f80      s5:0xffffffff803cc6c0
       s6:0xffffffff803cc6a8      s7:0xffffffff803cc690
       t8:0x0000000000000002      t9:0x0000005555a3bc98
       k0:0x0000000000000000      k1:0x0000000000000000
       gp:0x0000000120020460      sp:0x000000ffff899d70
       s8:0x000000ffff899d80      ra:0x0000000120006c1c
       sr:0x000000000400fff3      lo:0xdf3b645a1cac08c9
       hi:0x000000000000007f     bad:0x000000555589ba84
    cause:0x0000000000800020      pc:0x0000005555a3bcb4
```

表 5-1 コマンド出力

フィールド	説明
Crashed PID	クラッシュプロセスのIDです。
Crash signal	クラッシュを引き起こした信号です。 • **SIGABRT**—中断です。 • **SIGBUS**—バスエラーです。 • **SIGFPE**—間違った四則演算です。 • **SIGILL**—不正なハードウェア指令です。 • **SIGQUIT**—コントロール端末によってquit信号が送信されました。 • **SIGSEGV**—不正なメモリアクセスです。 • **SIGSYS**—不正なシステムコールです。

フィールド	説明
	• **SIGTRAP**—トラップメッセージです。 • **SIGXCPU**—CPU使用率の制限が超過しました。 • **SIGXFSZ**—ファイルサイズの制限が超過しました。 • **SIGUNKNOW**—不明な理由です。
Crash time	コアファイルが作成された時間です。
Core file path	コアファイルが保存されているディレクトリです。
Backtrace stopped	すべてのスタック情報が表示されています。

関連コマンド

reset exception context

5.1.2 display exception filepath

Syntax

display exception filepath

View

すべての view

定義済みユーザロール

network-admin

説明

display exception filepath コマンドはコアファイルのディレクトリを表示します。

例

MPU 上にあるコアファイルのディレクトリを表示します。

<AP> display exception filepath

```
The exception filepath is flash:.
```

5.1.3 exception filepath

Syntax

exception filepath *directory*

undo exception filepath *directory*

デフォルト

コアファイルのファイルは flash:/に保存されます。

View

User view

定義済みユーザロール

network-admin

パラメータ

directory: コアファイルを保存するディレクトリを指定します。

説明

exception filepath コマンドはコアファイルを保存するディレクトリを設定します。

undo exception filepath コマンドは指定されたディレクトリを削除します。

ディレクトリはマスタ装置のフラッシュのルートディレクトリのみ可能です。

システムは指定したディレクトリのコアディレクトリにコアファイルを保存します。コアディレクトリが存在しない場合、保存する前にコアディレクトリを作成します。

ディレクトリが指定されていない、あるいは指定されたディレクトリがアクセス不能である場合、プロセス例外のコアファイルを記録することができません。

例

コアファイルを保存するディレクトリを flash:/に指定します。

<AP> exception filepath flash:/

関連コマンド

- **display exception filepath**
- **process core**

5.1.4 process core

Syntax

process core { **maxcore** *value* | **off** } { **job** *job-id* | **name** *process-name* }

View

User view

デフォルト

プロセスは最初の例外のコアファイルを作成し、続く例外のコアファイルを作成しません。

定義済みユーザロール

network-admin

パラメータ

off: コアファイルの作成を無効にします。

maxcore *value*: コアファイルの作成を有効にし、コアファイルの最大数を設定します。設定範囲は 1～10 です。

name *process-name*: プロセス名を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別しません。

job *job-id*: job ID でプロセスを指定します。設定範囲は 1～2147483647 です。プロセスを再起動しても、job ID は変わりません。

説明

process core コマンドは例外のコアファイルを作成するプロセスを有効あるいは無効にし、コアファイルの最大数を設定します。

process core コマンドはプロセスのすべてのインスタンスに適用します。

コマンドは、コアファイルが最大数になるまで、指定されたプロセスがクラッシュするたびに、コアファイルを作成することを有効にします。コアファイルは例外情報を記録します。

コアファイルがシステム記憶リソースを消費するため、例外情報のレビューする必要がないプロセスはコアファイルの生成を無効にすることができます。

例

プロセス **routed** のコアファイルの作成を無効にします。

<AP> process core off name routed

プロセス **routed** のコアファイルの作成を有効にし、コアファイルの最大数を 5 に設定します。

<AP> process core maxcore 5 name routed

関連コマンド

- **display exception context**
- **exception filepath**

5.1.5 reset exception context

Syntax

reset exception context

View

User view

定義済みユーザロール

network-admin

説明

reset exception context コマンドはプロセス例外のコンテキスト情報を削除します。

例

プロセス例外のコンテキスト情報を削除します。

<AP> reset exception context

関連コマンド

display exception context

目次

このセクションのページは **15-x-x** です。

6 章 NetMeister 6-1
6.1 Netmeister 設定コマンド 6-1
6.1.1 display netmeister 6-1
6.1.2 netmeister account 6-4
6.1.3 netmeister alarm enable notice 6-6
6.1.4 netmeister enable 6-7
6.1.5 netmeister event log enable 6-8
6.1.6 netmeister management ip 6-9
6.1.7 netmeister mode 6-10
6.1.8 netmeister parent ip 6-11
6.1.9 netmeister parent-mode mqtt port 6-13
6.1.10 netmeister parent-mode sitename 6-14
6.1.11 netmeister proxy 6-15
6.1.12 netmeister update 6-17
6.1.13 netmeister track 6-18

6章 NetMeister

6.1 Netmeister設定コマンド

6.1.1 display netmeister

Syntax

display netmeister

View

すべての view

定義済みユーザロール

network-admin

説明

display netmeister コマンドは NetMeister 及び親機との接続情報を表示します。

例

子機モードの装置で NetMeisetr 及び親機との接続情報を表示します。

<Switch> display netmeister

```
NetMeister state                              : Enabled
Mode                                           : Child
Connection state with NetMeister              : Connected
Account name                                  : nec
Proxy information:
  State                                  : Connected
  URL                                   : http://www.abc.com:8080
  Username                              : admin
Parent 1:
  IP address                                  : 192.168.0.254
  Port number                                 : 443
  Connection state                            : Connected
Parent 2:
  IP address                                  : 192.168.0.255
  Port number                                 : 8443
  Connection state                            : Connected
```

親機モードの装置で NetMeisetr との接続情報を表示します。

<Switch> display netmeister

```
NetMeister state                          : Enabled
Mode                                       : Parent
Connection state with NetMeister          : Connected
Account name                               : nec
Proxy information:
State                                     :  --
Parent information:
Site name                                 : test
Interval                                  : 3600 sec
MQTT interval                             : 60 sec
MQTT status                               : Connected
```

表 6-1 コマンド出力

フィールド	説明
NetMeister state	NetMeister機能の状態です。 ● **Enabled** —有効 ● **Disabled** —無効
Mode	NetMeisterへの接続モードです。 ● **Parent** —親機モード ● **Child** —子機モード
Connection state with NetMeister	NetMeisterとの接続状況です。 ● **Connected.**—接続 ● **Disconnected.**—切断
Account name	グループIDです。
Proxy information	NetMeisterプロキシサーバとの接続に関する情報です。
State	プロキシサーバへの接続状態です。 ● **Connected.**—接続 ● **Disconnected.**—切断 ● **"--"** —プロキシサーバを設定していない場合に表示されます。
URL	プロキシサーバのURL。形式はhttp :// <domain>:<ポート>です。 domainはプロキシサーバのWebアドレスまたはIPアドレス、 portはポート番号です。 プロキシサーバが構成されていない場合、このフィールドは表示されません。

フィールド	説明
IP address	親機のIPアドレスです。 子機モード時のみ表示されます。
Port number	親機のポート番号です。 子機モード時のみ表示されます。
Connection state	NetMeister機能による親機への接続状態です。 ● **Connected.**—接続 ● **Disconnected.**—切断 子機モード時のみ表示されます。
Site name	拠点名です。 親機モード時のみ表示されます。
Interval	親機の更新情報の送信間隔です。 親機モード時のみ表示されます。
MQTT interval	MQTTプロトコルの送信間隔です。 親機モード時のみ表示されます。
MQTT status	MQTTプロトコルの接続状態です。 ● **Connected.**—接続 ● **Disconnected.**—切断 ● **"--"** —接続が成功しなかった場合に表示されます。 親機モード時のみ表示されます。

関連コマンド

- **netmeister account**
- **netmeister enable**
- **netmeister parent**

6.1.2 netmeister account

Syntax

netmeister account *account* **password** { **cipher** *cipherPassword* | **simple** *plainPassword* }

undo netmeister account

デフォルト

設定なし

View

System-view

定義済みユーザロール

network-admin

パラメータ

account: グループ ID を 2～31 文字の文字列で設定します。文字列に使用できるのは小文字、数字、およびハイフン(-)のみで、ハイフン(-)で開始または終了することはできません。

cipher: 暗号テキストのパスワードを設定します。

cipherPassword: 暗号化形式のパスワードを 41～73 文字の文字列で設定します。

simple: プレーンテキストのパスワードを設定します。セキュリティのため、プレーンテキストで設定されたパスワードを含めたすべてのパスワードは、暗号化されて保存されます。

plainPassword: プレーンテキスト形式のパスワードを 8～31 文字の文字列で設定します。文字列には、文字、数字、および!#$%&'()*+,-。/:;<=>@[]^_`{|}~の特殊文字のみを使用できます。文字列には、少なくとも 1 つの文字と 1 桁の数字を含める必要があります。

説明

netmeister account コマンドは親機への子機認証と NetMeister への装置登録で使用するグループ ID とパスワードを設定します。

undo netmeister account コマンドは設定したグループ ID とパスワードを削除します。

netmeister account コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister account コマンドを複数回実行した場合、最新の設定が有効になります。

NetMeister 上で、グループ ID とパスワードがあらかじめ設定されていることを確認して下さい。親機モードの場合、設定するグループ ID とパスワードが、NetMeister のグループ ID とパスワードと同じであることを確認してください。子機モードの場合、親機で設定されているグループ ID とパスワードも同じであることを確認してください。

例

親機への子機認証と NetMeister への装置登録のために、グループ ID **nec** とプレーンテキストのパスワード **nec1234** を装置に設定します。

<Switch> system-view

[Switch] netmeister account nec password simple nec1234

関連コマンド

- **netmeister enable**
- **display netmeister**

6.1.3 netmeister alarm enable notice

🕮 **メモ:**

netmeister alarm enable notice コマンドは Version 7.5.105 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister alarm enable notice

undo netmeister alarm enable notice

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister alarm enable notice コマンドによって NetMeister の注意レベルのアラーム

生成を有効にします。

undo netmeister alarm enable notice コマンドによって NetMeister の注意レベルの

NetMeister アラーム生成を無効にします。

この機能により、システムは次のイベントの注意レベルのアラームを生成できます。

- Telnet、ssh などを使用してログインまたはログアウトした場合
- 設定を保存した場合
- 設定を保存しないまま 5 分が経過した場合

例

NetMeister の注意レベルのアラームの生成を有効にします。

<Switch> system-view

[Switch] netmeister alarm enable notice

6.1.4 netmeister enable

Syntax

netmeister enable

undo netmeister enable

デフォルト

無効

View

System-view

定義済みユーザロール

network-admin

説明

netmeister enable コマンドは NetMeister 機能を有効にします。

undo netmeister enable コマンドは NetMeister 機能を無効に戻します。

例

NetMeister 機能を有効にします。

<Switch> system-view

[Switch] netmeister enable

6.1.5 netmeister event log enable

Syntax

netmeister event log enable

undo netmeister event log enable

View

System-view

デフォルト

有効

定義済みユーザロール

network-admin

説明

netmeister event log enable コマンドは NetMeister 機能が有効な時、端末がアソシエーションフェーズまたは認証フェーズで接続に失敗した際のイベントログを 5 分間隔で NetMeister に通知します。

undo netmeister event log enable コマンドはイベントログの送信を停止します。

netmeister event log enable コマンドは **netmeister enable** が有効な状態でも変更できます。

例

イベントログの送信を停止する。

<Switch> system-view

[Switch] undo netmeister event log enable

関連コマンド

netmeister enable

6.1.6 netmeister management ip

🕮 **メモ:**

netmeister management ip コマンドは Version 7.5.105 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister management ip *ip-address*

undo netmeister management ip

View

System-view

デフォルト

無効

定義済みユーザロール

network-admin

説明

netmeister management ip コマンドによって NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを設定します。

undo netmeister management ip コマンドによってデフォルトに戻します。

NetMeister 機能については NetMeister が提供している操作ガイドを参照してください。

例

NetMeister 機能[閉域網でリモートログインする]で表示する管理用 IP アドレスを 10.1.1.10 に設定します。

<Sysname> system-view

[Sysname] netmeister management ip 10.1.1.10

6.1.7 netmeister mode

Syntax

netmeister mode parent

undo netmeister mode parent

View

System-view

デフォルト

子機モード

定義済みユーザロール

network-admin

説明

netmeister mode parent コマンドを利用して NetMeister への接続モード親機モードにします。

親機モードは NetMeister 機能を有する親機ルータがいない環境において、NetMeisterPrime(有償サービス)を利用して NetMeister で管理する場合に利用します。NetMeister 機能を有する親機ルータがある環境では、それらの機器を親機とし、子機モードで利用して下さい。

undo netmeister mode parent コマンドを利用して NetMeister への接続モードを子機モードに戻します。

netmeister mode parent コマンドを設定する前に、**netmeister enable** や子機モード時に利用する **netmeister parent ip** コマンドが無効になっていることを確認してください。

例

NetMeister 機能を有する親機ルータがいない環境で QX を NetMeister によって管理するために、親機モードを設定します。

<Switch> system-view

[Switch] netmeister mode parent

関連コマンド

- **netmeister enable**
- **display netmeister**

6.1.8 netmeister parent ip

Syntax

netmeister parent ip *ip-address* [**port** *port-number*]

undo netmeister parent ip *ip-address*

View

System-view

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

ip *ip-address*: 親機の IP アドレスを設定します。

port *port-number*: 親機のポート番号を 1～65535 の範囲で設定します。デフォルトのポート番号は 443 です。

説明

netmeister parent ip コマンドは子機モードとして NetMeister に接続する際に、親機とする機器の IP アドレスとポート番号を設定します。

undo netmeister parent ip コマンドは子機として接続する親機の IP アドレスとポート番号を削除します。

netmeister parent ip コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister parent ip コマンドと **netmeister account** コマンドを設定し、**netmeister enable** コマンドを有効にすると、子機は認証応答を受信するまで親機に子機認証の要求を送信します。**netmeister parent ip** コマンドが複数設定されている場合、装置は設定されたすべてのアドレスに要求を送信し、それぞれの親機との接続を確立します。これにより、親機の障害によるサービスの中断を防ぎ、ネットワークの可用性が向上します。最大で 2 つまで親機 IP アドレスを設定できます。

例

IP アドレス **192.168.0.254** ポート番号 443 の親機に接続する子機として設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.0.254 port 443

IP アドレス **192.168.1.254** の親機に接続する子機として設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.1.254

関連コマンド

- **netmeister enable**
- **display netmeister**

6.1.9 netmeister parent-mode mqtt port

Syntax

netmeister parent-mode mqtt port [8883 | 443]

undo netmeister mode parent

View

System-view

デフォルト

8883

定義済みユーザロール

network-admin

説明

netmeister parent-mode mqtt port コマンドを利用して親機モードの QX が NetMeister に接続する際の MQTT プロトコルのポート番号を変更します。

undo netmeister mode parent コマンドを利用して NetMeister に接続する際の MQTT プロトコルのポート番号をデフォルトに戻します。

例

NetMeister に接続するためにネットワーク環境で 8883 を開放する必要がない様に、MQTT のポート番号を 443 に変更します。

<Switch> system-view

[Switch] netmeister parent-mode mqtt port 443

関連コマンド

- **netmeister enable**
- **display netmeister**

6.1.10 netmeister parent-mode sitename

Syntax

netmeister parent-mode sitename *name*

undo netmeister parent-mode sitename

View

System-view

デフォルト

なし

定義済みユーザロール

network-admin

説明

netmeister parent-mode sitename コマンドを利用して親機モードの QX が NetMeister に接続する際の拠点名を設定します。

undo netmeister mode parent コマンドを利用して拠点名の設定を削除します。

例

親機モードで NetMeister に接続するために拠点名 test を設定します。

<Switch> system-view

[Switch] netmeister parent-mode sitename test

関連コマンド

- **netmeister enable**
- **display netmeister**

6.1.11 netmeister proxy

Syntax

netmeister proxy url *url* [**username** *username* **password** { **cipher | simple** } *string*]

undo netmeister proxy

View

System-view

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

url *url*:プロキシサーバの URL を指定します。***http://***<*domain*>*:*<*port*>形式で、大文字と小文字を区別して 8 から 128 文字の文字列を指定します。<*domain*>引数はプロキシサーバのドメイン名または IP アドレスを表し、<*port*>引数は 1 から 65535 の範囲のポート番号を表します。デフォルトのポート番号は 80 です。

username *username*:プロキシサーバへのアクセスに使用するユーザー名を指定します。1 から 31 文字の大文字と小文字が区別されます。文字列には、バックスラッシュ (¥) 、引用符 (") 、疑問符 (?) 、スペースを含めることはできません。。

password:プロキシサーバへのアクセスに使用するパスワードを指定します。

cipher:パスワードを暗号化形式で指定します。

simple:プレーンテキスト形式でパスワードを指定します。セキュリティ上の理由から、プレーンテキスト形式で指定されたパスワードは暗号化形式で保存されます。

string:パスワード文字列を指定します。プレーンテキスト形式は、大文字と小文字を区別する 1 から 31 文字の文字列です。暗号化された形式は、大文字と小文字を区別した 33 から 73 文字の文字列です。プレーンテキストのパスワードには、バックスラッシュ、引用符 (") 、疑問符 (?) 、またはスペースを含めることはできません。

説明

netmeister proxy コマンドは装置が NetMeister 宛の https 通信のために指定された proxy サーバを利用します。親機への https 通信にはプロキシサーバを使用しません。

undo netmeister proxy コマンドはプロキシサーバの指定を削除します。

netmeister proxy コマンドを設定する前に、**netmeister enable** が無効になっていることを確認してください。

netmeister proxy 複数回実行した場合、最新の設定が有効になります。

例

IP アドレス **192.168.1.254** の親機に接続する子機とし、NetMeister にはプロキシサーバ 10.1.1.254 (ポート:8080)を使用するように設定します。

<Switch> system-view

[Switch] netmeister parent ip 192.168.1.254

[Switch] netmeister proxy url http://10.1.1.254:8080

関連コマンド

- **netmeister enable**
- **display netmeister**

6.1.12 netmeister update

🕮 メモ:

netmeister update コマンドは Version 7.5.105 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister update

View

User view

System-view

定義済みユーザロール

network-admin

説明

netmeister update コマンドは NetMeister に登録している装置情報を即時更新します。

例

装置名を変更した後、NetMeister に登録している装置情報を即時更新します。

<AP> system-view

[AP] sysname test

[AP] netmeister update

6.1.13 netmeister track

🕮 **メモ:**

netmeister track コマンドは Version 7.5.105 を含む以降のソフトウェアからサポートしています。

Syntax

netmeister track *track-entry-number*

undo netmeister track *track-entry-number*

View

System-view

デフォルト

設定なし

定義済みユーザロール

network-admin

パラメータ

track *track-entry-number*: 1～1024 の範囲の番号で指定されたトラックエントリに NetMeister 機能を紐付けます。

説明

netmeister track コマンドは、トラックエントリを NetMeister 機能に関連付けます。

undo netmeister track コマンドは、NetMeister 機能 とトラック エントリの関連付けを解除します。

本コマンドは NetMeister から Ping 監視設定をした場合に自動で設定されます。NetMeister から Ping 監視設定を削除した場合に自動で設定が解除されます。

本コマンドが適用されるトラックエントリは以下の条件と一致する NQA エントリのみです。NetMeister から Ping 監視設定をした場合、本条件と一致する設定が行われます。

- **nqa entry** コマンドで設定された *admin-name* は **nm-ping** である必要があります。
- **type** コマンドで設定された NQA テストタイプは **icmp-echo** である必要があります。
- **reaction checked-element probe-fail** コマンドでリアクションエントリが設定されている必要があります。

QX-W610 アクセスポイント

コマンドマニュアル

16. 高可用性

本マニュアルは以下に示す章で構成されています。

01-Track

目次

このセクションのページは **16-x-x** です。

1 章 Track 1-1
1.1 Track 設定コマンド 1-1
1.1.1 display track 1-1
1.1.2 object 1-5
1.1.3 track interface 1-6
1.1.4 track interface protocol 1-7
1.1.5 track list boolean 1-8
1.1.6 track nqa 1-9

1章 Track

1.1 Track設定コマンド

> 🕮 **メモ：**
>
> Track の設定は、ソフトウェアバージョン 7.5.105 を含む以降のソフトウェアからサポートしています。

display track

Syntax

display track { *track-entry-number* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

all: すべての track エントリの情報を表示します。

説明

display track コマンドは track エントリの情報を表示します。

例

すべての track エントリの情報を表示します。

<AP> display track all

```
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 7 seconds
  Tracked object type: NQA
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object：
    NQA entry: admin test
    Reaction: 10
```

```
    Remote IP/URL: 2.2.2.2
    Local IP: 1.1.1.1
    Interface: GigabitEthernet1/0/1
  Tracked by:
    Track-list 6
    Track-list 7
Track ID: 2
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked object:
    Interface:  Vlan-interface3
    Protocol: IPv4
  Tracked by:
    Track-list 6
    Track-list 7
Track ID: 3
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Percentage threshold list
  Notification delay: Positive 20, Negative 30 (in seconds)
  Threshold: Positive 40, Negative 30
  Percentage of positive objects: 50%
  Tracked objects:
    Object 1: Positive
    Object 3: Negative
Track ID: 4
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Weight threshold list
  Notification delay: Positive 20, Negative 30 (in seconds)
  Threshold: Positive 50, Negative 30
  Positive weight/total weight: 50/80
  Tracked objects:
    Object 1: Positive, Weight: 50
Object 3: Negative, Weight: 30
Track ID: 5
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: Boolean and list
  Notification delay: Positive 20, Negative 30 (in seconds)
  Tracked objects:
    Object 1: Positive
```

```
Object 3: Negative(not)
Object 10: NotReady(not)
```

表 1-1 コマンド出力

フィールド	説明
Track ID	trackエントリのIDです。
State	trackエントリの状態です。 • **Positive**—正常にtrackオブジェクトが動作しています。 • **NotReady**—trackオブジェクトが無効です。 • **Negative**—trackオブジェクトが異常です。
Duration	trackエントリが状態を保持する時間間隔です。
Type	trackのオブジェクトタイプです。 • Interface. • NQA. • List このフィールドは、**display track brief**コマンドが実行された場合にのみ表示されます。
Tracked object type	trackのオブジェクトタイプです。 • Interface. • NQA. • Boolean and list • Boolean or list • Percentage threshold list. • Weight threshold list.
Notification delay: Positive 20, Negative 30 (in seconds)	• trackモジュールは、trackエントリ状態が20秒の遅延時間後、Positiveに変更するとアプリケーションモジュールに通知します。 • trackモジュールは、trackエントリ状態が30秒の遅延時間後、Negativeに変更するとアプリケーションモジュールに通知します。
Threshold: Positive 40, Negative 30	ポジティブおよびネガティブ状態のしきい値です。 このフィールドは、trackのオブジェクトタイプが **Percentage threshold list** または **Weight threshold list** の場合にのみ表示されます。
Percentage of positive objects	trackリスト内のポジティブオブジェクトの割合です。 このフィールドは、trackのオブジェクトタイプが **Percentage threshold list** の場合にのみ表示されます。

フィールド	説明
Positive weight/total weight: 50/80	trackリスト内のすべてのオブジェクトの総Weightに対するポジティブオブジェクトの割合です。 このフィールドは、trackのオブジェクトタイプが **Weight threshold list** の場合にのみ表示されます。
Tracked object	trackエントリに関連づけられたtrackオブジェクトです。
NQA entry	trackエントリに関連づけられたNQAオペレーションです。
Reaction	trackエントリに関連づけられたリアクションエントリです。
IP route	trackエントリに関連づけられたルートです。
Remote IP/URL	リモートIPアドレスまたはURLです。リモートIPアドレスまたはURLが存在しない場合、2つの連続したハイフン（-）が表示されます。
Local IP	ローカルIPアドレスです。ローカルIPアドレスが存在しない場合、2つの連続するハイフン（-）が表示されます。
Interface	モニタ対象のインタフェースです。インタフェースをモニタしない場合は、2つの連続したハイフン（-）が表示されます。
Protocol	ルートのプロトコルタイプです。ルートが存在しないとき、**N/A**を表示します。
Nexthop interface	ルートのネクストホップです。ルートが存在しないとき、**N/A**を表示します。
Object 10 : Positive	trackのオブジェクトの状態です。 • Positive • NotReady • Negative trackのオブジェクトタイプが **Weight threshold list** の場合、オブジェクトのWeightも表示されます。 **（not）**属性が表示されている場合、trackリストはオブジェクトの状態をネガティブにします。
Tracked by	他のtrackエントリです。 オブジェクトタイプがtrackリストである場合、このフィールドは表示されません。

関連コマンド

- **track interface**
- **track interface protocol**
- **track nqa**

1.1.2 object

Syntax

object *track-entry-number* **[not]**

undo object *track-entry-number*

デフォルト

設定なし

View

Track view

定義済みユーザロール

network-admin

パラメータ

track-entry-number : track エントリの ID を指定します。設定範囲は 1～1024 です。

not：Track オブジェクトの状態を反転して判別します。オブジェクトが Positive 状態の場合、Track リストは Negative 状態とみなします。オブジェクトが Negative 状態の場合、Track リストは Positive 状態とみなします。このキーワードは Boolean リストでのみサポートされます。

説明

object コマンドは、track リストに track エントリをオブジェクトとして登録します。

undo track コマンドは、track リストからオブジェクトを削除します。

オブジェクトの Track エントリの ID には、追加先の Track リストの ID を指定することはできません。

Track リストには、最大 16 個のオブジェクトを追加できます。

下記の例のように、Track エントリ間のループとなる設定はできません。

(例)

Track List 1 : object 3 (Track 3)

Track List 2 : object 1 (Track 1)

Track List 3 : object 2 (Track 2)

例

#Boolean AND リストの Track 100 を作成し、Track 1 と Track 2 を Track オブジェクトとして登録します。

<AP> system-view

[AP] track 100 list boolean and

[AP-track-100] object 1

[AP-track-100] object 2

関連コマンド

track list boolean

1.1.3 track interface

Syntax

track *track-entry-number* **interface** *interface-type interface-number*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

説明

track interface コマンドは、インタフェースのリンク状態を監視する Track エントリを作成し、track entry view に移行するか、既存の track entry view に移行します。

undo track コマンドは、Track エントリとすべての設定を View から削除します。

Track エントリを作成するには、track オブジェクトタイプを示す **interface** パラメータを指定する必要があります。

既存の track entry view に移行するには、**track** *track-entry-number* コマンドを使用します。track オブジェクトタイプは必須ではありません。

track エントリの設定を変更するには、**undo track** コマンドを実行して track エントリを削除し、**track interface** コマンドを再度実行します。

インタフェースのリンクステータスを監視する track エントリの場合、track エントリの状態は次のように変化します。

- インタフェースのリンク状態が up である場合、track エントリの状態は Positive です。
- インタフェースのリンク状態が down である場合、track エントリの状態は Negative です。

インタフェースのリンク状態を表示する場合、**display ip interface brief** コマンドを使用します。

例

track エントリ 1 を作成して、VLAN インタフェース 10 のリンク状態を監視し、track entry view に移行します。

<AP> system-view

[AP] track 1 interface vlan-interface 10

[AP-track-1]

関連コマンド

- **display track**
- **display ip interface brief (コマンドマニュアルのセクション 4 *ネットワーク*)**

1.1.4 track interface protocol

Syntax

track *track-entry-number* **interface** *interface-type interface-number* **protocol** { **ipv4** }

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

interface-type interface-number: インタフェースのタイプと番号を指定します。

ipv4: IPv4 プロトコル状態をモニタします。インタフェースの IPv4 プロトコル状態が up である場合、track エントリの状態は Positive です。インタフェースの IPv4 プロトコル状態が down である場合、track エントリの状態は Negative です。インタフェースの IPv4 プロトコル状態を表示する場合、**display ip interface brief** コマンドを使用します。

説明

track interface protocol コマンドは、インタフェースのプロトコル状態を監視する track エントリを作成し、track entry view に移行するか、既存の track entry view に移行します。

undo track コマンドを使用して、track エントリとすべての設定を View から削除します。

track エントリを作成するには、track オブジェクトタイプを示す **interface protocol** パラメータを指定する必要があります。

既存の track entry view に移行するには、**track** *track-entry-number* コマンドを使用します。track オブジェクトタイプは必須ではありません。

track エントリの設定を変更するには、**undo track** コマンドを実行して track エントリを削除し、**track interface protocol** コマンドを再度実行します。

例

track エントリ 1 を作成して、VLAN インタフェース 2 の IPv4 プロトコル状態を監視し、track entry view に移行します。

<AP> system-view

[AP] track 1 interface vlan-interface 2 protocol ipv4

[AP-track-1]

関連コマンド

- **display track**
- **display ip interface brief (コマンドマニュアルのセクション 4 *ネットワーク*)**

1.1.5 track list boolean

Syntax

track *track-entry-number* **list boolean { and | or }**

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

and : Boolean の AND 演算を使用して Track リストの状態を判別します。

or : Boolean の OR 演算を使用して Track リストの状態を判別します。

説明

track list boolean コマンドは、Boolean リストの Track エントリを作成し、track entry view に移行するか、既存の Boolean リストの track entry view に移行します。

undo track コマンドは、track エントリとすべての設定を View から削除します。

Boolean リストは、Boolean ロジックに基づいた Track オブジェクトのリストです。 さらに次のタイプに分類できます。

- Boolean AND リスト ー リストに登録されたすべての Track オブジェクトが Positive 状態の場合に Positive 状態となります。 いずれかの Track オブジェクトが Negative 状態にある場合は Negative 状態となります。
- Boolean OR リスト ー リストに登録されたいずれかの Track オブジェクトが Positive 状態の場合に Positive 状態となります。 すべての Track オブジェクトが Negative 状態の場合は Negative 状態となります。

例

Boolean OR リストの track エントリ 1 を作成し、track entry view に移行します。

<AP> system-view

[AP] track 1 list boolean or

[AP-track-1]

関連コマンド

- **display track**
- **object**

1.1.6 track nqa

Syntax

track *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-number*

undo track *track-entry-number*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

track-entry-number: track エントリの ID を指定します。設定範囲は 1～1024 です。

entry *admin-name operation-tag*: track エントリに関連づけられる NQA オペレーションを指定します。*admin-name* は NQA オペレーションを作成する NQA オペレーションの管理者名です。設定範囲は 1～32 文字です。大文字、小文字を区別しません。*operation-tag* は NQA オペレーションのタグです。設定範囲は 1～32 文字です。大文字、小文字を区別しません。

reaction *item-number*: track エントリに関連づけられるリアクションエントリを指定します。*item-number* はリアクションエントリの ID です。設定範囲は 1～10 です。

説明

track nqa コマンドを使用して、NQA 操作のリアクションを監視する track エントリを作成し track entry view に移行するか、既存の track entry view に移行します。

undo nqa コマンドを使用して、track エントリとすべての設定を View から削除します。

track エントリを作成するには、track オブジェクトタイプを示す **nqa** パラメータを指定する必要があります。

既存の track entry view に移行するには、**track** *track-entry-number* コマンドを使用します。track オブジェクトタイプは必須ではありません。

track エントリの設定を変更するには、**undo track** コマンドを実行して track エントリを削除し、**track nqa** コマンドを再度実行します。

例

track エントリ 1 を作成して、NQA テスト admin-test のリアクションエントリ 3 を監視し、track entry view に移行します。

<AP> system-view

[AP] track 1 nqa entry admin test reaction 3

[AP-track-1]

関連コマンド

display track